

## デバイスコンプライアンス(サンプル) - 詳細

デバイス コンプライアンス レポートでは、デバイスレベルのアクセス ポリシーへのコンプライアンスに関する要約情報が示されます。  
このレポートには、選択したデバイスに関するコンプライアンス メトリクスと、スコープ中のすべての違反に関する情報が表示されます。  
このレポートには、指定したデバイスのコンプライアンス メトリクスと、スコープ中のすべての違反に関する詳細情報が表示されます。このレポートはポリシーが指定のデバイスに適用されているかどうかを把握するのに役立ちます。また、デバイスの問題のあるアクセス設定を検出するのに効果があります。

このレポートのスコープ : Public Policy

1. デバイス別コンプライアンス - 要約	2
2. デバイスの詳細と違反	3
3. デバイス別のコンプライアンス - 詳細	9
4. レポートプロパティ	63

## 1. デバイス別コンプライアンス - 要約

55% コンプライアンス (106 件中 58 件のテスト)

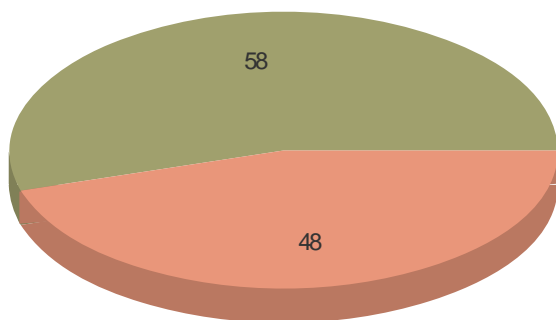
スコープ内のテスト総数: 106

ポリシー違反の総数: 48

重大なポリシー違反の数: 3

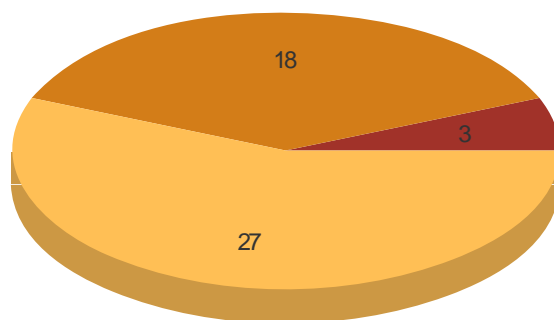
ポリシー最終計算日時: 2008/05/27 10:45:45 JST

コンプライアンス別のデバイス  
テスト



■ コンプライアンス ■ 非コンプライアンス


重要度別のデバイス違反



■ 重大 ■ 高 ■ 中

## 2. デバイスの詳細と違反

このセクションには、各デバイスの違反 (非コンプライアンスのアクセス テスト) が表示されます。

 [main FW \[192.169.1.1\] - 55% コンプライアンス](#)

### デバイス : main FW

IP アドレス: 192.169.1.1  
 ファイアウォールタイプ: ファイアウォール  
 コンプライアンス: 55%  
 最終計算時間: 08/05/27

#### ACL ルールセット: ACCESS

#	ソース	宛先	サービス	アクション	方向
1	192.170.1.97, 192.169.1.1, 200.160.2.1, 16.0.0.1	任意	任意		インバウンド
2	任意	192.170.33.0 - 192.170.33.255	TCP/80, UDP/53, TCP/53, TCP/21, TCP/443, TCP/25		インバウンド
3	200.160.1.0 - 200.160.1.255, 200.160.2.0 - 200.160.2.255	192.170.33.0 - 192.170.33.255	任意		インバウンド
4	192.170.18.0 - 192.170.18.255, 192.170.17.0 - 192.170.17.255, 192.170.16.0 - 192.170.16.255, ...	任意	任意		インバウンド
5	任意	200.160.1.0 - 200.160.1.255, 200.160.2.0 - 200.160.2.255	任意		インバウンド
6	192.170.35.0 - 192.170.35.255, 192.170.36.0 - 192.170.36.255, 192.170.34.0 - 192.170.34.255, ...	200.160.1.0 - 200.160.1.255, 200.160.2.0 - 200.160.2.255	UDP/69		インバウンド
7	任意	192.170.18.0 - 192.170.18.255, 192.170.17.0 - 192.170.17.255, 192.170.16.0 - 192.170.16.255, ...	TCP/21, TCP/23		インバウンド
8	192.170.27.0 - 192.170.27.255, 192.170.26.0 - 192.170.26.255, 192.170.25.0 - 192.170.25.255	任意	任意		インバウンド
9	192.170.36.0 - 192.170.36.255	192.170.21.0 - 192.170.21.255	TCP/80, UDP/135, TCP/135		インバウンド
10	192.170.21.0 - 192.170.21.255	192.170.36.0 - 192.170.36.255	UDP/69		インバウンド
11	200.160.1.0 - 200.160.1.255	192.170.36.2 - 192.170.36.41, 192.170.36.0 - 192.170.36.255	TCP/443, TCP/135		インバウンド
12	192.170.18.0 - 192.170.18.255, 192.170.17.0 - 192.170.17.255, 192.170.16.0 - 192.170.16.255, ...	192.170.35.0 - 192.170.35.255, 192.170.36.0 - 192.170.36.255	TCP/21		インバウンド
13	192.170.25.0 - 192.170.25.255	192.170.34.0 - 192.170.34.255	TCP/135		インバウンド
14	192.170.33.0 - 192.170.33.255	192.170.27.0 - 192.170.27.255	TCP/8500		インバウンド
15	192.170.1.97, 192.169.1.1, 200.160.2.1, 16.0.0.1	任意	任意		アウトバウンド
16	任意	任意	任意		インバウンド
17	任意	任意	任意		インバウンド



デバイス違反

ルールタイプ	!	新規	テストID	ソース	宛先	サービス	APR 名
	<b>C</b>		31	Internet (外部)	int15 (内部サーバ)	[23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - ...	ログインサービスのブロック
	<b>C</b>		688	int18 (パートナー)	int2809 (DMZ)	4/ICMP, 8/ICMP, 12/ICMP	ICMPエコーメッセージのブロック
	<b>C</b>		714	VPN (パートナー)	int2809 (DMZ)	4/ICMP, 8/ICMP, 12/ICMP	ICMPエコーメッセージのブロック
	<b>H</b>		144	int2809 (DMZ)	int15 (内部サーバ)	[23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - ...	ログインサービスのブロック
	<b>H</b>		158	int2809 (DMZ)	int15 (内部サーバ)	[135/TCP,135/UDP] - loc-srv, [137/UDP,137/TCP] - netbios-ns, [138/UDP] - netbios-dgm, [139/TCP] - ...	Windows NetBIOSのブロック
	<b>H</b>		686	int18 (パートナー)	int2809 (DMZ)	'4553' [21227/TCP,21317/TCP], accessremotepc [34012/TCP], agent_40421 [30/TCP,40421/TCP], anig ...	トロイ/ワームポートのブロック
	<b>H</b>		689	int18 (パートナー)	int2809 (DMZ)	[37/TCP,37/UDP] - time, 1-20/TCP, 1-20/UDP	スモールサービスのブロック
	<b>H</b>		693	int18 (パートナー)	int2809 (DMZ)	[111/TCP,111/UDP] - sunrpc, [2049/TCP,2049/UDP,100003/RPC] - nfs, nlockmgr ...	RPCとNFSのブロック
	<b>H</b>		696	int18 (パートナー)	int2809 (DMZ)	[135/TCP,135/UDP] - loc-srv, [137/UDP,137/TCP] - netbios-ns, [138/UDP] - netbios-dgm, [139/TCP] - ...	Windows NetBIOSのブロック
	<b>H</b>		700	int18 (パートナー)	int2809 (DMZ)	6000-6255/TCP	X-Windowsのブロック
	<b>H</b>		702	int18 (パートナー)	int15 (内部サーバ)	[23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - ...	ログインサービスのブロック
	<b>H</b>		704	int18 (パートナー)	int2809 (DMZ)	[23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - ...	ログインサービスのブロック



ルールタイプ	!	新規	テストID	ソース	宛先	サービス	APR 名
			705	int18 (パートナー)	int2809 (DMZ)	[1080/TCP,1080/UDP] - socks, [119/TCP] - nntp, [123/UDP] - ntp, [161/TCP,161/UDP] - snmp, [162/UDP] ...	その他のサービスのブロック
			710	VPN (パートナー)	int2809 (DMZ)	4553 [21227/TCP,21317/TCP], accessremotepc [34012/TCP], agent_40421 [30/TCP,40421/TCP], anig ...	トロイ/ワームポートのブロック
			715	VPN (パートナー)	int2809 (DMZ)	[37/TCP,37/UDP] - time, 1-20/TCP, 1-20/UDP	スモールサービスのブロック
			719	VPN (パートナー)	int2809 (DMZ)	[111/TCP,111/UDP] - sunrpc, [2049/TCP,2049/UDP,100003/RPC] - nfs, nlockmgr ...	RPCとNFSのブロック
			722	VPN (パートナー)	int2809 (DMZ)	[135/TCP,135/UDP] - loc-srv, [137/UDP,137/TCP] - netbios-ns, [138/UDP] - netbios-dgm, [139/TCP] - ...	Windows NetBIOSのブロック
			726	VPN (パートナー)	int2809 (DMZ)	6000-6255/TCP	X-Windowsのブロック
			728	VPN (パートナー)	int15 (内部サーバ)	[23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - ...	ログインサービスのブロック
			730	VPN (パートナー)	int2809 (DMZ)	[23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - ...	ログインサービスのブロック
			731	VPN (パートナー)	int2809 (DMZ)	[1080/TCP,1080/UDP] - socks, [119/TCP] - nntp, [123/UDP] - ntp, [161/TCP,161/UDP] - snmp, [162/UDP] ...	その他のサービスのブロック
			3	Internet (外部)	int2809 (DMZ)	[25/TCP] - smtp	SMTPアクセスの制限
			5	Internet (外部)	int2809 (DMZ)	[443/TCP,8443/TCP] - https, [80/TCP,8080/TCP] - http	HTTPアクセスの制限
			7	Internet (外部)	int2809 (DMZ)	[53/UDP] - domain_u, [53/TCP] - domain_t	DNSアクセスの制限
			27	Internet (外部)	int2809 (DMZ)	任意	アクセス制限 - 宛先
			94	Internet (外部)	int15 (内部サーバ)	任意	アクセスのブロック
			200	int2809 (DMZ)	int15 (内部サーバ)	任意	アクセス制限 - 宛先

ルールタイプ	!	新規	テストID	ソース	宛先	サービス	APR 名
			<a href="#">220</a>	int15 (内部サーバ)	Internet (外部)	isakmp [500/TCP,500/UDP], l2tpd [1701/TCP,1701/UDP], pptp [1723/TCP], Any/ESP, Any/GRE	VPN アクセスのブロック
			<a href="#">227</a>	int15 (内部サーバ)	Internet (外部)	任意	アクセスのブロック
			<a href="#">229</a>	int15 (内部サーバ)	int2809 (DMZ)	[23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwddgen, [512/TCP] - exec, [513/TCP] - ...	ログイン サービスのブロック
			<a href="#">236</a>	int15 (内部サーバ)	int2809 (DMZ)	[111/TCP,111/UDP] - sunrpc, [2049/TCP,2049/UDP,100003/RPC] - nfs, nlockmgr ...	RPCとNFSのブロック
			<a href="#">243</a>	int15 (内部サーバ)	int2809 (DMZ)	6000-6255/TCP	X-Windowsのブロック
			<a href="#">250</a>	int15 (内部サーバ)	int2809 (DMZ)	[37/TCP,37/UDP] - time, 1-20/TCP, 1-20/UDP	スモール サービスのブロック
			<a href="#">257</a>	int15 (内部サーバ)	int2809 (DMZ)	[1080/TCP,1080/UDP] - socks, [119/TCP] - nntp, [123/UDP] - ntp, [161/TCP,161/UDP] - snmp, [162/UDP] ...	その他のサービスのブロック
			<a href="#">264</a>	int15 (内部サーバ)	int2809 (DMZ)	'4553' [21227/TCP,21317/TCP], accessremotepc [34012/TCP], agent_40421 [30/TCP,40421/TCP], anig ...	トロイ/ワーム ポートのブロック
			<a href="#">271</a>	int15 (内部サーバ)	int2809 (DMZ)	0/ICMP, 3/ICMP, 4/ICMP, 11/ICMP, 12/ICMP	ICMP応答メッセージのブロック
			<a href="#">278</a>	int15 (内部サーバ)	int2809 (DMZ)	任意	アクセス制限 - 宛先
			<a href="#">285</a>	int15 (内部サーバ)	int2809 (DMZ)	任意	アクセス制限 - サービス
			<a href="#">691</a>	int18 (パートナー)	int2809 (DMZ)	任意	アクセス制限 - サービス
			<a href="#">694</a>	int18 (パートナー)	int15 (内部サーバ)	任意	アクセス制限 - 宛先
			<a href="#">703</a>	int2809 (DMZ)	int18 (パートナー)	任意	アクセスのブロック
			<a href="#">707</a>	int15 (内部サーバ)	int18 (パートナー)	任意	アクセスのブロック
			<a href="#">708</a>	int18 (パートナー)	int2809 (DMZ)	任意	アクセス制限 - 宛先
			<a href="#">717</a>	VPN (パートナー)	int2809 (DMZ)	任意	アクセス制限 - サービス
			<a href="#">720</a>	VPN (パートナー)	int15 (内部サーバ)	任意	アクセス制限 - 宛先
			<a href="#">729</a>	int2809 (DMZ)	VPN (パートナー)	任意	アクセスのブロック
			<a href="#">733</a>	int15 (内部サーバ)	VPN (パートナー)	任意	アクセスのブロック

ルールタイプ	!	新規	テストID	ソース	宛先	サービス	APR 名
			734	VPN (パートナー)	int2809 (DMZ)	任意	アクセス制限 - 宛先

### 3. デバイス別のコンプライアンス - 詳細

ここでは、違反のプロパティやアクセス結果を含む各違反についての詳細が表示されます。

**C** 違反 31: Internet (外部) -> int15 (内部サーバ)

APR: ログイン サービスのブロック

外部ゾーンと内部サーバゾーン間のログインサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるログインサービス(Telnet、SSHなど)は使用すべきではありません。ログインサービスを使用するとリモート管理が可能になるため、信頼できるソースからのログインサービスのみを許可してください。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int15 )

ソース: Internet (外部)

宛先: int15 (内部サーバ)

サービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shell

APR 経路: Public Policy/外部アクセス/外部 ~ 内部サーバ/ログイン サービスのブロック

追加日時: 2007/05/24 18:10:56 JST

説明: デバイスマインFWで、ソース Internet (外部)と宛先int15 (内部サーバ)の間にアクセスが見つかりました。APRでは、任意のサービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP, 129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shell のソースと宛先の間でアクセスを使用できないように指定されています。次のIPアドレスとポートが宛先にアクセスできます:  
768 IP アドレス:  
192.170.17.0-192.170.19.255

1 ポート:  
23 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
23 (TCP)	main FW (int15 )	192.170.17.0-192.170.19.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int15 )	192.170.17.0-192.170.19.255	23 (TCP)

**C** 違反 714: VPN (パートナー) -> int2809 (DMZ)

APR: ICMPエコー メッセージのブロック

パートナーゾーンとDMZゾーン間のICMPエコーメッセージはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるICMPエコーメッセージ(Echo Requestなど)は使用すべきではありません。ICMPエコーメッセージは、サイバー攻撃の基本であるネットワークの偵察行為の一部として使用される可能性があります。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: VPN (パートナー)

宛先: int2809 (DMZ)

サービス: 4/ICMP, 8/ICMP, 12/ICMP

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/ICMPエコーメッセージのブロック

追加日時: 2007/02/17 19:48:30 JST

説明: デバイスmain FWで、ソースVPN (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。APR では、任意のサービス: 4/ICMP, 8/ICMP, 12/ICMPのソースと宛先の間でアクセスを使用できないように指定されています。次のIPアドレスとポートが宛先にアクセスできます:  
256 IP アドレス:  
192.170.33.0-192.170.33.255

3 ポート:  
4 (ICMP)  
8 (ICMP)  
12 (ICMP)

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
4 (ICMP), 8 (ICMP), 12 (ICMP)	main FW (int2809)	192.170.33.0-192.170.33.255

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.33.0-192.170.33.255	4 (ICMP), 8 (ICMP), 12 (ICMP)

**C** 違反 688: int18 (パートナー) -> int2809 (DMZ)

APR: ICMPエコー メッセージのブロック

パートナーゾーンとDMZゾーン間のICMPエコーメッセージはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるICMPエコーメッセージ(Echo Requestなど)は使用すべきではありません。ICMPエコーメッセージは、サイバー攻撃の基本であるネットワークの偵察行為の一部として使用される可能性があります。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int18 (パートナー)

宛先: int2809 (DMZ)

サービス: 4/ICMP, 8/ICMP, 12/ICMP

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/ICMPエコーメッセージのブロック

追加日時: 2007/02/17 19:48:32 JST

説明: デバイスmain FWで、ソース int18 (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。APR では、任意のサービス: 4/ICMP, 8/ICMP, 12/ICMP のソースと宛先の間でアクセスを使用できないように指定されています。次の IP アドレス と ポート が宛先にアクセスできます:  
256 IP アドレス:  
192.170.33.0-192.170.33.255

3 ポート:  
4 (ICMP)  
8 (ICMP)  
12 (ICMP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
4 (ICMP), 8 (ICMP), 12 (ICMP)	main FW (int2809)	192.170.33.0-192.170.33.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.33.0-192.170.33.255	4 (ICMP), 8 (ICMP), 12 (ICMP)

**H** 違反 158: int2809 (DMZ) -> int15 (内部サーバ)

APR: Windows NetBIOSのブロック

DMZゾーンと内部サーバゾーン間のWindows NetBIOSサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるWindows NetBIOSサービスは使用すべきではありません。その理由は、これらのサービスが数多くの脆弱性を持つことが分かっているためです。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int15 )

ソース: int2809 (DMZ)

宛先: int15 (内部サーバ)

サービス: [135/TCP,135/UDP] - loc-srv, [137/UDP,137/TCP] - netbios-ns, [138/UDP] - netbios-dgm, [139/TCP] - netbios-ssn, [445/TCP,445/UDP] - microsoft-ds

APR 経路: Public Policy/DMZアクセス/DMZ ~ 内部サーバ/Windows NetBIOSのブロック

追加日時: 2007/02/06 20:57:23 JST

説明: デバイスmain FWで、ソースint2809 (DMZ)と宛先int15 (内部サーバ)の間にアクセスが見つかりました。APRでは、任意のサービス: [135/TCP, 135/UDP] - loc-srv, [137/UDP, 137/TCP] - netbios-ns, [138/UDP] - netbios-dgm, [139/TCP] - netbios-ssn, [445/TCP, 445/UDP] - microsoft-ds のソースと宛先の間でアクセスを使用できないように指定されています。次のIPアドレスとポートが宛先にアクセスできます:  
256 IP アドレス:  
192.170.21.0-192.170.21.255

2 ポート:  
135 (UDP)  
135 (TCP)

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
135 (TCP), 135 (UDP)	main FW (int15 )	192.170.21.0-192.170.21.255

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int15 )	192.170.21.0-192.170.21.255	135 (TCP), 135 (UDP)

**H** 違反 726: VPN (パートナー) -> int2809 (DMZ)

APR: X-Windowsのブロック

パートナーゾーンとDMZゾーン間のX-Windowsサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるX-Windowsサービスは使用すべきではありません。X-Windowsサービスを使用するとリモート管理が可能になるため、信頼できるソースからのX-Windowsサービスのみを許可してください。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: VPN (パートナー)

宛先: int2809 (DMZ)

サービス: 6000-6255/TCP

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/X-Windowsのブロック

追加日時: 2007/02/17 19:48:30 JST

説明: デバイスmain FWで、ソース VPN (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。APR では、サービス 6000-6255/TCP のソースと宛先の間でアクセスを使用できないように指定されています。次の IP アドレス と ポート が宛先にアクセスできます:  
256 IP アドレス:  
192.170.33.0-192.170.33.255

256 ポート:  
6000-6255 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
6000-6255 (TCP)	main FW (int2809)	192.170.33.0-192.170.33.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.33.0-192.170.33.255	6000-6255 (TCP)

**H** 違反 704: int18 (パートナー) -> int2809 (DMZ)

APR: **ログイン サービスのブロック**

パートナーゾーンとDMZゾーン間のログインサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるログインサービス(Telnet、SSHなど)は使用すべきではありません。ログインサービスを使用するとリモート管理が可能になるため、信頼できるソースからのログインサービスのみを許可してください。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int18 (パートナー)

宛先: int2809 (DMZ)

サービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shell

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/ログインサービスのブロック

追加日時: 2007/02/17 19:48:32 JST

説明: デバイスmain FWで、ソース int18 (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。APR では、任意のサービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP, 129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shell のソースと宛先の間でアクセスを使用できないように指定されています。次の IP アドレス と ポート が宛先にアクセスできます:  
256 IP アドレス:  
192.170.33.0-192.170.33.255

7 ポート:  
129 (UDP)  
22-23 (TCP)  
512-514 (TCP)  
129 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
22-23 (TCP), 129 (TCP), 512-514 (TCP), 129 (UDP)	main FW (int2809)	192.170.33.0-192.170.33.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.33.0-192.170.33.255	22-23 (TCP), 129 (TCP), 512-514 (TCP), 129 (UDP)

**H** 違反 715: VPN (パートナー) -> int2809 (DMZ)  
 APR: **スモール サービスのブロック**

パートナーゾーンとDMZゾーン間のスモールサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるスモールサービスグループは使用すべきではありません。その理由は、これらのサービスが数多くの脆弱性を持つことが分かっているためです。

タイプ: 潜在するエンティティに対するアクセスルールなし  
 アクセス結果: ✖ アクセスが存在  
 テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809 )  
 ソース: VPN (パートナー)  
 宛先: int2809 (DMZ)  
 サービス: [37/TCP,37/UDP] - time, 1-20/TCP, 1-20/UDP

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/スモールサービスのブロック  
 追加日時: 2007/02/17 19:48:30 JST

説明: デバイスmain FWで、ソースVPN (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。  
 APR では、任意のサービス: [37/TCP, 37/UDP] - time, 1-20/TCP, 1-20/UDPのソースと宛先の間でアクセスを使用できないように指定されています。  
 次の IP アドレス と ポート が宛先にアクセスできます:  
 256 IP アドレス:  
 192.170.33.0-192.170.33.255

42 ポート:  
 1-20 (UDP)  
 1-20 (TCP)  
 37 (UDP)  
 37 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
1-20 (TCP), 37 (TCP), 1-20 (UDP), 37 (UDP)	main FW (int2809 )	192.170.33.0-192.170.33.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809 )	192.170.33.0-192.170.33.255	1-20 (TCP), 37 (TCP), 1-20 (UDP), 37 (UDP)

**H** 違反 693: int18 (パートナー) -> int2809 (DMZ)

APR: RPCとNFSのブロック

パートナーゾーンとDMZゾーン間のRPCサービスとNFSサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるRPCサービスとNFSサービスは使用すべきではありません。その理由は、これらのサービスが数多くの脆弱性を持つことが分かっているためです。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int18 (パートナー)

宛先: int2809 (DMZ)

サービス: [111/TCP,111/UDP] - sunrpc, [2049/TCP,2049/UDP,100003/RPC] - nfs, nlockmgr [100021/RPC,4045/TCP,4045/UDP]

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/RPCとNFSのブロック

追加日時: 2007/02/17 19:48:32 JST

説明: デバイスmain FWで、ソース int18 (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。  
APR では、任意のサービス:[111/TCP, 111/UDP] - sunrpc, [2049/TCP, 2049/UDP, 100003/RPC] - nfs, nlockmgr [100021/RPC, 4045/TCP, 4045/UDP]のソースと宛先の間でアクセスを使用できないように指定されています。  
次の IP アドレス と ポート が宛先にアクセスできます:  
256 IP アドレス:  
192.170.33.0-192.170.33.255

6 ポート:  
4045 (TCP)  
4045 (UDP)  
111 (UDP)  
111 (TCP)  
2049 (UDP)  
2049 (TCP)

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
111 (TCP), 2049 (TCP), 4045 (TCP), 111 (UDP), 2049 (UDP), 4045 (UDP)	main FW (int2809)	192.170.33.0-192.170.33.255

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.33.0-192.170.33.255	111 (TCP), 2049 (TCP), 4045 (TCP), 111 (UDP), 2049 (UDP), 4045 (UDP)

**H** 違反 705: int18 (パートナー) -> int2809 (DMZ)

APR: その他のサービスのブロック

パートナーゾーンとDMZゾーン間の他のサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間で、このサービスグループは使用すべきではありません。その理由は、これらのサービスが数多くの脆弱性を持つことが分かっているためです。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int18 (パートナー)

宛先: int2809 (DMZ)

サービス: [1080/TCP,1080/UDP] - socks, [119/TCP] - nntp, [123/UDP] - ntp, [161/TCP,161/UDP] - snmp, [162/UDP] - snmptrap, [514/UDP] - syslog, [515/TCP] - printer, [69/UDP] - tftp, [79/TCP] - finger

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/その他のサービスのブロック

追加日時: 2007/02/17 19:48:32 JST

説明: デバイスマインFWで、ソースint18(パートナー)と宛先int2809(DMZ)の間にアクセスが見つかりました。APRでは、任意のサービス:[1080/TCP, 1080/UDP] - socks, [119/TCP] - nntp, [123/UDP] - ntp, [161/TCP, 161/UDP] - snmp, [162/UDP] - snmptrap, [514/UDP] - syslog, [515/TCP] - printer, [69/UDP] - tftp, 1以上のソースと宛先の間でアクセスを使用できないように指定されています。次のIPアドレスとポートが宛先にアクセスできます:  
256 IP アドレス:  
192.170.33.0-192.170.33.255

14 ポート:  
123 (TCP)  
79 (TCP)  
161 (TCP)  
9050 (UDP)  
9050 (TCP)  
1080 (UDP)  
119 (TCP)  
69 (UDP)  
514 (UDP)  
515 (TCP)  
3 以上

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
79 (TCP), 119 (TCP), 123 (TCP), 161 (TCP), 515 (TCP), 1080 (TCP), 9050 (TCP), 69 (UDP), 123 (UDP), ...	main FW (int2809)	192.170.33.0-192.170.33.255

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.33.0-192.170.33.255	79 (TCP), 119 (TCP), 123 (TCP), 161 (TCP), 515 (TCP), 1080 (TCP), 9050 (TCP), 69 (UDP), 123 (UDP), ...

**H** 違反 702: int18 (パートナー) -> int15 (内部サーバ)

APR: **ログイン サービスのブロック**

パートナーゾーンと内部サーバゾーン間のログインサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるログインサービス(Telnet、SSHなど)は使用すべきではありません。ログインサービスを使用するとリモート管理が可能になるため、信頼できるソースからのログインサービスのみを許可してください。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int15)

ソース: int18 (パートナー)

宛先: int15 (内部サーバ)

サービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shell

APR 経路: Public Policy/パートナーアクセス/パートナー～内部サーバ/ログインサービスのブロック

追加日時: 2007/02/17 19:48:32 JST

説明: デバイスmain FWで、ソース int18 (パートナー)と宛先int15 (内部サーバ)の間にアクセスが見つかりました。APR では、任意のサービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP, 129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shell のソースと宛先の間でアクセスを使用できないように指定されています。次の IP アドレス と ポート が宛先にアクセスできます:  
768 IP アドレス:  
192.170.17.0-192.170.19.255  
  
1 ポート:  
23 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
23 (TCP)	main FW (int15)	192.170.17.0-192.170.19.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int15)	192.170.17.0-192.170.19.255	23 (TCP)

**H** 違反 144: int2809 (DMZ) -> int15 (内部サーバ)

APR: **ログイン サービスのブロック**

DMZゾーンと内部サーバゾーン間のログインサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるログインサービス(Telnet、SSHなど)は使用すべきではありません。ログインサービスを使用するとリモート管理が可能になるため、信頼できるソースからのログインサービスのみを許可してください。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int15)

ソース: int2809 (DMZ)

宛先: int15 (内部サーバ)

サービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shell

APR 経路: Public Policy/DMZアクセス/DMZ ~ 内部サーバ/ログイン サービスのブロック

追加日時: 2007/02/06 20:57:23 JST

説明: デバイスマain FWで、ソース int2809 (DMZ)と宛先int15 (内部サーバ)の間にアクセスが見つかりました。APR では、任意のサービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP, 129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shell のソースと宛先の間でアクセスを使用できないように指定されています。次の IP アドレス と ポート が宛先にアクセスできます:  
768 IP アドレス:  
192.170.17.0-192.170.19.255  
  
1 ポート:  
23 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
23 (TCP)	main FW (int15)	192.170.17.0-192.170.19.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int15)	192.170.17.0-192.170.19.255	23 (TCP)

**H** 違反 710: VPN (パートナー) -> int2809 (DMZ)

APR: トロイ/ワーム ポートのブロック

パートナーゾーンとDMZゾーン間のトロイ/ワーム  
ポートはブロックする必要があります。NIST公開仕様800-41によれば、このグループのポートはワ  
ームとトロイによって使用されることが分かっているため、ブロックする必要があります。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: VPN (パートナー)

宛先: int2809 (DMZ)

サービス: '4553' [21227/TCP,21317/TCP], accessremotepc [34012/TCP], agent\_40421  
[30/TCP,40421/TCP], anig [5190/TCP], aok [8961/TCP], aol-admin  
[30029/TCP], asylum [23432/TCP], attackftp [666/TCP], Backdoor.Akak  
[4321/TCP], Backdoor.Emcommander [31337/TCP], Backdoor.Hale  
[6351/TCP,5555/TCP,48522/TCP], BackOrifice [31337/UDP], bagel  
[6777/TCP], beagle.b [8866/TCP], beagle.e [2745/TCP], beagle.j [2745/TCP],  
beagle.m [2556/TCP], beagle.u [4751/TCP], beagle.w [2535/TCP], beagle.x  
[2535/TCP], biggluck [34324/TCP], bind-shell [33270/TCP], bionet [12349/TCP],  
blaster [4444/TCP], blazer5 [5000/TCP], bo2k [54320/TCP,54321/UDP], bofra  
[1639/TCP,1640/TCP], bolgi [5732/TCP], bugbear [36794/TCP], bugs  
[2115/TCP], bunker\_hill [61348/TCP,61603/TCP,63485/TCP], Cdk  
[15858/TCP,79/TCP], chupacabra [13473/TCP,20203/TCP], coma  
[10607/TCP], connection [8720/TCP,60411/TCP,60412/TCP], crazzynet  
[17499/TCP,17500/TCP], dabber  
[9898/TCP,9899/TCP,9900/TCP,9901/TCP,9999/TCP], dagger  
[2589/TCP,1386/TCP], death [2/TCP], deepthroat  
[2140/UDP,3150/UDP,6670/TCP,6771/TCP,60000/TCP], deltasource  
[6883/TCP], Dipnet [11768/TCP,15118/TCP], doom\_backdoor [10167/UDP],  
drat [48/TCP,50/TCP], event-horizon [4488/TCP], evilftp [12346/TCP], Explet  
[1250/TCP], fluxay [10/TCP], forced-entry [1025/TCP,9999/TCP], freak88  
[7001/UDP,31337/UDP], frenzy [1257/TCP], Gaobot Backdoor  
[1749/TCP,63809/TCP], Gaobot Backward [22226/TCP,13659/TCP],  
gatecrasher [6969/TCP], girlfriend [21554/TCP], glacier [7626/TCP],  
globe\_backdoor [28876/TCP], hackatack [31785/TCP,31789/UDP,31791/UDP],  
helemoo [28876/TCP], host-control [11051/TCP], Huayu [887/TCP], HVL-RAT  
[1095/TCP,1097/TCP,1098/TCP,1099/TCP], incommand [9400/TCP], ingreslock  
[1524/TCP,1524/UDP], jade [1024/TCP,65421/TCP], Janx [5533/TCP], Kibuv  
[5300/TCP,420/TCP], Kibuv-ftp [9604/TCP,7955/TCP], Kipis.L [5311/TCP],  
knooth.e [11040/TCP], kuang2 [17300/TCP], lateda [9999/TCP], Linux OSF  
[29369/TCP,29369/UDP], Linux.Plupii [7222/UDP], lion  
[6008/TCP,33567/TCP,33568/TCP], litmus [30005/TCP], lovgate  
[10168/TCP,6000/TCP], mantis [37237/TCP], matrix  
[1269/TCP,1025/UDP,1025/TCP], millenium [20000/TCP,20001/TCP],  
mstream\_agent [10498/UDP,7983/UDP], mstream\_handler  
[6723/TCP,15104/TCP,12754/TCP], mydoom  
[3127/TCP,3198/TCP,1034/TCP,10080/TCP,1042/TCP,1080/TCP], MySQL Bot  
[2301/TCP,2304/TCP], Mytob.AI [10087/TCP], Mytob.AJ [61137/TCP],  
Mytob.AR [10089/TCP], Mytob.BB Backdoor [10155/TCP], Mytob.BB Backward  
[10487/TCP], Mytob.BH [12187/TCP], Mytob.BL [10085/TCP], Mytob.CM  
[10082/TCP], Mytob.FX [10099/TCP], NetBus  
[12345/TCP,12346/TCP,20034/TCP], netdemon [15000/TCP], netmonitor  
[7300/TCP,7301/TCP,7306/TCP,7307/TCP,7308/TCP], Netsky  
[5556/TCP,5557/TCP], netsphere [30100/TCP,30102/TCP], netspy  
[1033/TCP], phatbot [4387/TCP], ... (71 - 追加サービス)

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/トロイ/ワーム  
ポートのブロック

追加日時: 2007/02/17 19:48:30 JST

説明:

デバイスmain FWで、ソース VPN (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。  
 APR では、任意のサービス:'4553' [21227/TCP, 21317/TCP], accessremotepc [34012/TCP], agent\_40421 [30/TCP, 40421/TCP], anig [5190/TCP], aok [8961/TCP], aol-admin [30029/TCP], asylum [23432/TCP], attackftp [666/TCP], 258 以上のソースと宛先の間でアクセスを使用できないように指定されています。  
 次の IP アドレス と ポート が宛先にアクセスできます:  
 256 IP アドレス:  
 192.170.33.0-192.170.33.255

246 ポート:  
 30100 (TCP)  
 6868 (TCP)  
 3150 (UDP)  
 1 (UDP)  
 21317 (TCP)  
 11768 (TCP)  
 65000 (TCP)  
 31789 (UDP)  
 2140 (UDP)  
 29369 (TCP)  
 197 以上

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
2 (TCP), 8 (TCP), 10 (TCP), 30 (TCP), 48 (TCP), 50 (TCP), 79 (TCP), 420-421 (TCP), 531 (TCP), 559 ...	main FW (int2809 )	192.170.33.0-192.170.33.255

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809 )	192.170.33.0-192.170.33.255	2 (TCP), 8 (TCP), 10 (TCP), 30 (TCP), 48 (TCP), 50 (TCP), 79 (TCP), 420-421 (TCP), 531 (TCP), 559 ...

**H** 違反 731: VPN (パートナー) -> int2809 (DMZ)

APR: その他のサービスのブロック

パートナーゾーンとDMZゾーン間の他のサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間で、このサービスグループは使用すべきではありません。その理由は、これらのサービスが数多くの脆弱性を持つことが分かっているためです。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: VPN (パートナー)

宛先: int2809 (DMZ)

サービス: [1080/TCP,1080/UDP] - socks, [119/TCP] - nntp, [123/UDP] - ntp, [161/TCP,161/UDP] - snmp, [162/UDP] - snmptrap, [514/UDP] - syslog, [515/TCP] - printer, [69/UDP] - tftp, [79/TCP] - finger

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/その他のサービスのブロック

追加日時: 2007/02/17 19:48:30 JST

説明: デバイスマain FWで、ソースVPN (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。APRでは、任意のサービス: [1080/TCP, 1080/UDP] - socks, [119/TCP] - nntp, [123/UDP] - ntp, [161/TCP, 161/UDP] - snmp, [162/UDP] - snmptrap, [514/UDP] - syslog, [515/TCP] - printer, [69/UDP] - tftp, 1以上のソースと宛先の間でアクセスを使用できないように指定されています。次のIPアドレスとポートが宛先にアクセスできます:  
256 IP アドレス:  
192.170.33.0-192.170.33.255

14 ポート:  
123 (TCP)  
79 (TCP)  
161 (TCP)  
9050 (UDP)  
9050 (TCP)  
1080 (UDP)  
119 (TCP)  
69 (UDP)  
514 (UDP)  
515 (TCP)  
3 以上

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
79 (TCP), 119 (TCP), 123 (TCP), 161 (TCP), 515 (TCP), 1080 (TCP), 9050 (TCP), 69 (UDP), 123 (UDP), ...	main FW (int2809)	192.170.33.0-192.170.33.255

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.33.0-192.170.33.255	79 (TCP), 119 (TCP), 123 (TCP), 161 (TCP), 515 (TCP), 1080 (TCP), 9050 (TCP), 69 (UDP), 123 (UDP), ...

**H** 違反 722: VPN (パートナー) -> int2809 (DMZ)

APR: Windows NetBIOSのブロック

パートナーゾーンとDMZゾーン間のWindows NetBIOSサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるWindows NetBIOSサービスは使用すべきではありません。その理由は、これらのサービスが数多くの脆弱性を持つことが分かっているためです。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: VPN (パートナー)

宛先: int2809 (DMZ)

サービス: [135/TCP, 135/UDP] - loc-srv, [137/UDP, 137/TCP] - netbios-ns, [138/UDP] - netbios-dgm, [139/TCP] - netbios-ssn, [445/TCP, 445/UDP] - microsoft-ds

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/Windows NetBIOSのブロック

追加日時: 2007/02/17 19:48:30 JST

説明: デバイスmain FWで、ソースVPN (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。APRでは、任意のサービス: [135/TCP, 135/UDP] - loc-srv, [137/UDP, 137/TCP] - netbios-ns, [138/UDP] - netbios-dgm, [139/TCP] - netbios-ssn, [445/TCP, 445/UDP] - microsoft-dsのソースと宛先の間でアクセスを使用できないように指定されています。次のIPアドレスとポートが宛先にアクセスできます:  
512 IP アドレス:  
192.170.33.0-192.170.33.255  
192.170.36.0-192.170.36.255

8 ポート:  
445 (TCP)  
135 (UDP)  
137-138 (UDP)  
137 (TCP)  
139 (TCP)  
445 (UDP)  
135 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
135 (TCP), 137 (TCP), 139 (TCP), 445 (TCP), 135 (UDP), 137-138 (UDP), 445 (UDP)	main FW (int2809)	192.170.33.0-192.170.33.255
135 (TCP)	main FW (int2809)	192.170.36.0-192.170.36.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.33.0-192.170.33.255	135 (TCP), 137 (TCP), 139 (TCP), 445 (TCP), 135 (UDP), 137-138 (UDP), 445 (UDP)
main FW (int2809)	192.170.36.0-192.170.36.255	135 (TCP)

**H** 違反 700: int18 (パートナー) -> int2809 (DMZ)

APR: X-Windowsのブロック

パートナーゾーンとDMZゾーン間のX-Windowsサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるX-Windowsサービスは使用すべきではありません。X-Windowsサービスを使用するとリモート管理が可能になるため、信頼できるソースからのX-Windowsサービスのみを許可してください。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int18 (パートナー)

宛先: int2809 (DMZ)

サービス: 6000-6255/TCP

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/X-Windowsのブロック

追加日時: 2007/02/17 19:48:32 JST

説明: デバイスmain FWで、ソース int18 (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。APR では、サービス 6000-6255/TCP のソースと宛先の間でアクセスを使用できないように指定されています。次の IP アドレス と ポート が宛先にアクセスできます:  
256 IP アドレス:  
192.170.33.0-192.170.33.255

256 ポート:  
6000-6255 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
6000-6255 (TCP)	main FW (int2809)	192.170.33.0-192.170.33.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.33.0-192.170.33.255	6000-6255 (TCP)

**H** 違反 719: VPN (パートナー) -> int2809 (DMZ)

APR: RPCとNFSのブロック

パートナーゾーンとDMZゾーン間のRPCサービスとNFSサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるRPCサービスとNFSサービスは使用すべきではありません。その理由は、これらのサービスが数多くの脆弱性を持つことが分かっているためです。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: VPN (パートナー)

宛先: int2809 (DMZ)

サービス: [111/TCP,111/UDP] - sunrpc, [2049/TCP,2049/UDP,100003/RPC] - nfs, nlockmgr [100021/RPC,4045/TCP,4045/UDP]

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/RPCとNFSのブロック

追加日時: 2007/02/17 19:48:30 JST

説明: デバイスmain FWで、ソースVPN (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。APR では、任意のサービス:[111/TCP, 111/UDP] - sunrpc, [2049/TCP, 2049/UDP, 100003/RPC] - nfs, nlockmgr [100021/RPC, 4045/TCP, 4045/UDP]のソースと宛先の間でアクセスを使用できないように指定されています。次のIPアドレスとポートが宛先にアクセスできます:  
256 IP アドレス:  
192.170.33.0-192.170.33.255

- 6 ポート:
- 4045 (TCP)
- 4045 (UDP)
- 111 (UDP)
- 111 (TCP)
- 2049 (UDP)
- 2049 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
111 (TCP), 2049 (TCP), 4045 (TCP), 111 (UDP), 2049 (UDP), 4045 (UDP)	main FW (int2809 )	192.170.33.0-192.170.33.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809 )	192.170.33.0-192.170.33.255	111 (TCP), 2049 (TCP), 4045 (TCP), 111 (UDP), 2049 (UDP), 4045 (UDP)

**H** 違反 728: VPN (パートナー) -> int15 (内部サーバ)

APR: **ログイン サービスのブロック**

パートナーゾーンと内部サーバゾーン間のログインサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるログインサービス(Telnet、SSHなど)は使用すべきではありません。ログインサービスを使用するとリモート管理が可能になるため、信頼できるソースからのログインサービスのみを許可してください。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int15)

ソース: VPN (パートナー)

宛先: int15 (内部サーバ)

サービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shell

APR 経路: Public Policy/パートナーアクセス/パートナー～内部サーバ/ログインサービスのブロック

追加日時: 2007/02/17 19:48:30 JST

説明: デバイスmain FWで、ソースVPN (パートナー)と宛先int15 (内部サーバ)の間にアクセスが見つかりました。APRでは、任意のサービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP, 129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shellのソースと宛先の間でアクセスを使用できないように指定されています。次のIPアドレスとポートが宛先にアクセスできます:  
768 IP アドレス:  
192.170.17.0-192.170.19.255  
  
1 ポート:  
23 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
23 (TCP)	main FW (int15)	192.170.17.0-192.170.19.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int15)	192.170.17.0-192.170.19.255	23 (TCP)

**H** 違反 696: int18 (パートナー) -> int2809 (DMZ)

APR: Windows NetBIOSのブロック

パートナーゾーンとDMZゾーン間のWindows NetBIOSサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるWindows NetBIOSサービスは使用すべきではありません。その理由は、これらのサービスが数多くの脆弱性を持つことが分かっているためです。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int18 (パートナー)

宛先: int2809 (DMZ)

サービス: [135/TCP,135/UDP] - loc-srv, [137/UDP,137/TCP] - netbios-ns, [138/UDP] - netbios-dgm, [139/TCP] - netbios-ssn, [445/TCP,445/UDP] - microsoft-ds

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/Windows NetBIOSのブロック

追加日時: 2007/02/17 19:48:32 JST

説明: デバイスmain FWで、ソース int18 (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。APR では、任意のサービス: [135/TCP, 135/UDP] - loc-srv, [137/UDP, 137/TCP] - netbios-ns, [138/UDP] - netbios-dgm, [139/TCP] - netbios-ssn, [445/TCP, 445/UDP] - microsoft-ds のソースと宛先の間でアクセスを使用できないように指定されています。次の IP アドレス と ポート が宛先にアクセスできます:  
512 IP アドレス:  
192.170.33.0-192.170.33.255  
192.170.36.0-192.170.36.255

8 ポート:  
445 (TCP)  
135 (UDP)  
137-138 (UDP)  
137 (TCP)  
139 (TCP)  
445 (UDP)  
135 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
135 (TCP), 137 (TCP), 139 (TCP), 445 (TCP), 135 (UDP), 137-138 (UDP), 445 (UDP)	main FW (int2809)	192.170.33.0-192.170.33.255
135 (TCP)	main FW (int2809)	192.170.36.0-192.170.36.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.33.0-192.170.33.255	135 (TCP), 137 (TCP), 139 (TCP), 445 (TCP), 135 (UDP), 137-138 (UDP), 445 (UDP)
main FW (int2809)	192.170.36.0-192.170.36.255	135 (TCP)

**H** 違反 689: int18 (パートナー) -> int2809 (DMZ)

APR: **スモール サービスのブロック**

パートナーゾーンとDMZゾーン間のスモールサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるスモールサービスグループは使用すべきではありません。その理由は、これらのサービスが数多くの脆弱性を持つことが分かっているためです。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int18 (パートナー)

宛先: int2809 (DMZ)

サービス: [37/TCP,37/UDP] - time, 1-20/TCP, 1-20/UDP

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/スモールサービスのブロック

追加日時: 2007/02/17 19:48:32 JST

説明: デバイスマインFWで、ソースint18(パートナー)と宛先int2809(DMZ)の間にアクセスが見つかりました。APRでは、任意のサービス:[37/TCP, 37/UDP] - time, 1-20/TCP, 1-20/UDPのソースと宛先の間でアクセスを使用できないように指定されています。次のIPアドレスとポートが宛先にアクセスできます:  
256 IP アドレス:  
192.170.33.0-192.170.33.255

42 ポート:  
1-20 (UDP)  
1-20 (TCP)  
37 (UDP)  
37 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
1-20 (TCP), 37 (TCP), 1-20 (UDP), 37 (UDP)	main FW (int2809)	192.170.33.0-192.170.33.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.33.0-192.170.33.255	1-20 (TCP), 37 (TCP), 1-20 (UDP), 37 (UDP)

**H** 違反 686: int18 (パートナー) -> int2809 (DMZ)

APR: トロイ/ワーム ポートのブロック

パートナーゾーンとDMZゾーン間のトロイ/ワーム  
ポートはブロックする必要があります。NIST公開仕様800-41によれば、このグループのポートはワ  
ームとトロイによって使用されることが分かっているため、ブロックする必要があります。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int18 (パートナー)

宛先: int2809 (DMZ)

サービス: '4553' [21227/TCP,21317/TCP], accessremotepc [34012/TCP], agent\_40421  
[30/TCP,40421/TCP], anig [5190/TCP], aok [8961/TCP], aol-admin  
[30029/TCP], asylum [23432/TCP], attackftp [666/TCP], Backdoor.Akak  
[4321/TCP], Backdoor.Emcommander [31337/TCP], Backdoor.Hale  
[6351/TCP,5555/TCP,48522/TCP], BackOrifice [31337/UDP], bagel  
[6777/TCP], beagle.b [8866/TCP], beagle.e [2745/TCP], beagle.j [2745/TCP],  
beagle.m [2556/TCP], beagle.u [4751/TCP], beagle.w [2535/TCP], beagle.x  
[2535/TCP], biggluck [34324/TCP], bind-shell [33270/TCP], bionet [12349/TCP],  
blaster [4444/TCP], blazer5 [5000/TCP], bo2k [54320/TCP,54321/UDP], bofra  
[1639/TCP,1640/TCP], bolgi [5732/TCP], bugbear [36794/TCP], bugs  
[2115/TCP], bunker\_hill [61348/TCP,61603/TCP,63485/TCP], Cdk  
[15858/TCP,79/TCP], chupacabra [13473/TCP,20203/TCP], coma  
[10607/TCP], connection [8720/TCP,60411/TCP,60412/TCP], crazzynet  
[17499/TCP,17500/TCP], dabber  
[9898/TCP,9899/TCP,9900/TCP,9901/TCP,9999/TCP], dagger  
[2589/TCP,1386/TCP], death [2/TCP], deepthroat  
[2140/UDP,3150/UDP,6670/TCP,6771/TCP,60000/TCP], deltasource  
[6883/TCP], Dipnet [11768/TCP,15118/TCP], doom\_backdoor [10167/UDP],  
drat [48/TCP,50/TCP], event-horizon [4488/TCP], evilftp [12346/TCP], Explet  
[1250/TCP], fluxay [10/TCP], forced-entry [1025/TCP,9999/TCP], freak88  
[7001/UDP,31337/UDP], frenzy [1257/TCP], Gaobot Backdoor  
[1749/TCP,63809/TCP], Gaobot Backward [22226/TCP,13659/TCP],  
gatecrasher [6969/TCP], girlfriend [21554/TCP], glacier [7626/TCP],  
globe\_backdoor [28876/TCP], hackatack [31785/TCP,31789/UDP,31791/UDP],  
helemoo [28876/TCP], host-control [11051/TCP], Huayu [887/TCP], HVL-RAT  
[1095/TCP,1097/TCP,1098/TCP,1099/TCP], incommand [9400/TCP], ingreslock  
[1524/TCP,1524/UDP], jade [1024/TCP,65421/TCP], Janx [5533/TCP], Kibuv  
[5300/TCP,420/TCP], Kibuv-ftp [9604/TCP,7955/TCP], Kipis.L [5311/TCP],  
knooth.e [11040/TCP], kuang2 [17300/TCP], lateda [9999/TCP], Linux OSF  
[29369/TCP,29369/UDP], Linux.Plupii [7222/UDP], lion  
[6008/TCP,33567/TCP,33568/TCP], litmus [30005/TCP], lovgate  
[10168/TCP,6000/TCP], mantis [37237/TCP], matrix  
[1269/TCP,1025/UDP,1025/TCP], millenium [20000/TCP,20001/TCP],  
mstream\_agent [10498/UDP,7983/UDP], mstream\_handler  
[6723/TCP,15104/TCP,12754/TCP], mydoom  
[3127/TCP,3198/TCP,1034/TCP,10080/TCP,1042/TCP,1080/TCP], MySQL Bot  
[2301/TCP,2304/TCP], Mytob.AI [10087/TCP], Mytob.AJ [61137/TCP],  
Mytob.AR [10089/TCP], Mytob.BB Backdoor [10155/TCP], Mytob.BB Backward  
[10487/TCP], Mytob.BH [12187/TCP], Mytob.BL [10085/TCP], Mytob.CM  
[10082/TCP], Mytob.FX [10099/TCP], NetBus  
[12345/TCP,12346/TCP,20034/TCP], netdemon [15000/TCP], netmonitor  
[7300/TCP,7301/TCP,7306/TCP,7307/TCP,7308/TCP], Netsky  
[5556/TCP,5557/TCP], netsphere [30100/TCP,30102/TCP], netspy  
[1033/TCP], phatbot [4387/TCP], ... (71 - 追加サービス)

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/トロイ/ワーム  
ポートのブロック

追加日時: 2007/02/17 19:48:32 JST

説明:

デバイスmain FWで、ソース int18 (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。  
 APR では、任意のサービス:'4553' [21227/TCP, 21317/TCP], accessremotepc [34012/TCP], agent\_40421 [30/TCP, 40421/TCP], anig [5190/TCP], aok [8961/TCP], aol-admin [30029/TCP], asylum [23432/TCP], attackftp [666/TCP], 258 以上のソースと宛先の間でアクセスを使用できないように指定されています。  
 次の IP アドレス と ポート が宛先にアクセスできます:  
 256 IP アドレス:  
 192.170.33.0-192.170.33.255

246 ポート:  
 30100 (TCP)  
 6868 (TCP)  
 3150 (UDP)  
 1 (UDP)  
 21317 (TCP)  
 11768 (TCP)  
 65000 (TCP)  
 31789 (UDP)  
 2140 (UDP)  
 29369 (TCP)  
 197 以上

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
2 (TCP), 8 (TCP), 10 (TCP), 30 (TCP), 48 (TCP), 50 (TCP), 79 (TCP), 420-421 (TCP), 531 (TCP), 559 ...	main FW (int2809 )	192.170.33.0-192.170.33.255

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809 )	192.170.33.0-192.170.33.255	2 (TCP), 8 (TCP), 10 (TCP), 30 (TCP), 48 (TCP), 50 (TCP), 79 (TCP), 420-421 (TCP), 531 (TCP), 559 ...

**H** 違反 730: VPN (パートナー) -> int2809 (DMZ)

APR: **ログイン サービスのブロック**

パートナーゾーンとDMZゾーン間のログインサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるログインサービス(Telnet、SSHなど)は使用すべきではありません。ログインサービスを使用するとリモート管理が可能になるため、信頼できるソースからのログインサービスのみを許可してください。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: VPN (パートナー)

宛先: int2809 (DMZ)

サービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shell

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/ログインサービスのブロック

追加日時: 2007/02/17 19:48:30 JST

説明: デバイスmain FWで、ソースVPN (パートナー)と宛先int2809 (DMZ)の間にアクセスが見つかりました。APR では、任意のサービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP, 129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shell のソースと宛先の間でアクセスを使用できないように指定されています。次の IP アドレス と ポート が宛先にアクセスできます:  
256 IP アドレス:  
192.170.33.0-192.170.33.255

7 ポート:  
129 (UDP)  
22-23 (TCP)  
512-514 (TCP)  
129 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
22-23 (TCP), 129 (TCP), 512-514 (TCP), 129 (UDP)	main FW (int2809)	192.170.33.0-192.170.33.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.33.0-192.170.33.255	22-23 (TCP), 129 (TCP), 512-514 (TCP), 129 (UDP)

**M** 違反 285: int15 (内部サーバ) -> int2809 (DMZ)  
 APR: アクセス制限 - サービス

内部サーバ  
 ゾーンとDMZゾーン間のアクセスは、宛先ポートが10個という制限を越えてはなりません。ネットワーク設計のベストプラクティスとして、アクセス制御をネットワークに適用することをお勧めします。この方針に従えば、ポートレベルのアクセス制御が確実に実現され、指定したポートのみにアクセスが許可されることとなります。

タイプ: 潜在的なエンティティに対するアクセスルール制限  
 アクセス結果: ✖ アクセス制限を超えました  
 テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809 )  
 ソース: int15 (内部サーバ)  
 宛先: int2809 (DMZ)  
 サービス: 任意

宛先ポートに対する制限: <=10 宛先ポート

APR 経路: Public Policy/内部サーバ アクセス/内部サーバ~DMZ/アクセス制限 - サービス  
 追加日時: 2007/02/06 20:57:22 JST

説明: デバイスマインFWで、宛先int2809 (DMZ)にアクセスできる宛先ポートが多すぎます。APRでは、10を超える宛先ポートが、宛先の各IPアドレスにアクセスできないように制限されています。次のIPアドレスが、アクセスできる宛先ポートの数を超過しています:  
 192.170.1.96-192.170.1.111 - 197119宛先ポートでアクセス可能です  
 192.170.33.0-192.170.36.255 - 197119宛先ポートでアクセス可能です

**⇒** アクセス可能なターゲット

指定された制限よりも多くのポートから到達できる IP 範囲

IP 範囲	ポート数	ポート範囲
main FW (int2809 ) {Addresses Behind:192.170.1.96-192.170.1.111,192.170.33.0-192.170.36.255}	197,119	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...
main FW (int2809 ) {Addresses Behind:192.170.1.96-192.170.1.111,192.170.33.0-192.170.36.255}	197,119	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...

**M** 違反 257: int15 (内部サーバ) -> int2809 (DMZ)

APR: その他のサービスのブロック

内部サーバ

ゾーンとDMZゾーン間の他のサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間で、このサービスグループは使用すべきではありません。その理由は、これらのサービスが数多くの脆弱性を持つことが分かっているためです。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int15 (内部サーバ)

宛先: int2809 (DMZ)

サービス: [1080/TCP,1080/UDP] - socks, [119/TCP] - nntp, [123/UDP] - ntp, [161/TCP,161/UDP] - snmp, [162/UDP] - snmptrap, [514/UDP] - syslog, [515/TCP] - printer, [69/UDP] - tftp, [79/TCP] - finger

APR 経路: Public Policy/内部サーバ  
アクセス/内部サーバ~DMZ/その他のサービスのブロック

追加日時: 2007/02/06 20:57:22 JST

説明: デバイスmain FWで、ソース int15 (内部サーバ)と宛先int2809 (DMZ)の間にアクセスが見つかりました。  
APR では、任意のサービス: [1080/TCP, 1080/UDP] - socks, [119/TCP] - nntp, [123/UDP] - ntp, [161/TCP, 161/UDP] - snmp, [162/UDP] - snmptrap, [514/UDP] - syslog, [515/TCP] - printer, [69/UDP] - tftp, 1 以上のソースと宛先の間でアクセスを使用できないように指定されています。  
次の IP アドレスとポートが宛先にアクセスできます:  
1040 IP アドレス:  
192.170.1.96-192.170.1.111  
192.170.33.0-192.170.36.255

14 ポート:  
123 (TCP)  
79 (TCP)  
161 (TCP)  
9050 (UDP)  
9050 (TCP)  
1080 (UDP)  
119 (TCP)  
69 (UDP)  
514 (UDP)  
515 (TCP)  
3 以上

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
79 (TCP), 119 (TCP), 123 (TCP), 161 (TCP), 515 (TCP), 1080 (TCP), 9050 (TCP), 69 (UDP), 123 (UDP), ...	main FW (int2809)	192.170.1.96-192.170.1.111
79 (TCP), 119 (TCP), 123 (TCP), 161 (TCP), 515 (TCP), 1080 (TCP), 9050 (TCP), 69 (UDP), 123 (UDP), ...	main FW (int2809)	192.170.33.0-192.170.36.255

📡 アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.1.96-192.170.1.111	79 (TCP), 119 (TCP), 123 (TCP), 161 (TCP), 515 (TCP), 1080 (TCP), 9050 (TCP), 69 (UDP), 123 (UDP), ...
main FW (int2809)	192.170.33.0-192.170.36.255	79 (TCP), 119 (TCP), 123 (TCP), 161 (TCP), 515 (TCP), 1080 (TCP), 9050 (TCP), 69 (UDP), 123 (UDP), ...

**M** 違反 703: int2809 (DMZ) -> int18 (パートナー)

APR: **アクセスのブロック**

DMZゾーンとパートナーゾーン間のアクセスは、すべてのサービスについてブロックする必要があります。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int18)

ソース: int2809 (DMZ)

宛先: int18 (パートナー)

サービス: 任意

APR 経路: Public Policy/DMZアクセス/DMZ ~ パートナー/アクセスのブロック

追加日時: 2007/02/26 15:28:18 JST

説明: デバイスマain FWで、ソース int2809 (DMZ)と宛先int18 (パートナー)の間にアクセスが見つかりました。APR では、任意のサービスのソースと宛先の間でアクセスを使用できないように指定されています。次の IP アドレス と ポート が宛先にアクセスできます:  
 255 IP アドレス:  
 200.160.2.0  
 200.160.2.2-200.160.2.255  
 1 ポート:  
 69 (UDP)

📡 アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
69 (UDP)	main FW (int18)	200.160.2.0
69 (UDP)	main FW (int18)	200.160.2.2-200.160.2.255

📡 アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int18)	200.160.2.0	69 (UDP)
main FW (int18)	200.160.2.2-200.160.2.255	69 (UDP)

**M** 違反 3: Internet (外部) -> int2809 (DMZ)

APR: SMTPアクセスの制限

外部ゾーンとDMZゾーン間のSMTPアクセスは、宛先IPが5個という制限を越えてはなりません。一般的なDMZ環境では、少数のSMTPサーバを使用すべきです。このルールに違反すると、ファイアウォールが正しく構成されず、不適切なSMTPアクセスにDMZがさらされる可能性があります。

タイプ: 潜在的なエンティティに対するアクセスルール制限

アクセス結果: ✖ アクセス制限を超えました

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: Internet (外部)

宛先: int2809 (DMZ)

サービス: [25/TCP] - smtp

宛先 IP に対する制限: <=5 宛先 IP アドレス

APR 経路: Public Policy/外部アクセス/外部 ~ DMZ/SMTPアクセスの制限

追加日時: 2007/02/06 20:57:21 JST

説明: デバイスmain FWで、宛先int2809 (DMZ)にアクセスできる IP アドレス数が多すぎます。  
APR では、5を超える宛先 IP アドレス が サービス [25/TCP] - smtp にアクセスできないように制限されています。  
次の IP アドレス が、アクセスできる IP アドレスの数を超過しています:

**⇒** アクセス可能なターゲット

指定された制限よりも多くの IP アドレスに到達できるポート範囲

ポート範囲	IP アドレスの数	IP 範囲
25 (TCP)	256	192.170.33.0-192.170.33.255

**M** 違反 27: Internet (外部) -> int2809 (DMZ)

APR: **アクセス制限 - 宛先**

外部ゾーンとDMZゾーン間のアクセスは、すべてのサービスの宛先IPが50個という制限を越えてはなりません。ネットワーク設計のベストプラクティスとして、アクセス制御をネットワークに適用することをお勧めします。この方針に従えば、宛先レベルのアクセス制御が確実に実現され、指定したIPアドレスのみにアクセスが許可されることとなります。

タイプ: 潜在的なエンティティに対するアクセスルール制限

アクセス結果: ✖ アクセス制限を超えました

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: Internet (外部)

宛先: int2809 (DMZ)

サービス: 任意

宛先 IP に対する制限: <=50 宛先 IP アドレス

APR 経路: Public Policy/外部アクセス/外部 ~ DMZ/アクセス制限 - 宛先

追加日時: 2007/02/06 20:57:21 JST

説明: デバイスmain FWで、宛先int2809 (DMZ)にアクセスできる IP アドレス数が多すぎます。  
APR では、50を超える宛先 IP アドレス が 任意のサービス にアクセスできないように制限されています。  
次の IP アドレス が、アクセスできる IP アドレスの数を超過しています:

**➡** アクセス可能なターゲット

指定された制限よりも多くの IP アドレスに到達できるポート範囲

ポート範囲	IP アドレスの数	IP 範囲
21 (TCP)	256	192.170.33.0-192.170.33.255
25 (TCP)	256	192.170.33.0-192.170.33.255
53 (TCP)	256	192.170.33.0-192.170.33.255
80 (TCP)	256	192.170.33.0-192.170.33.255
443 (TCP)	256	192.170.33.0-192.170.33.255
53 (UDP)	256	192.170.33.0-192.170.33.255

**M** 違反 733: int15 (内部サーバ) -> VPN (パートナー)  
 APR: アクセスのブロック

内部サーバ  
 ゾーンとパートナーゾーン間のアクセスは、すべてのサービスについてブロックする必要があります。

タイプ: 潜在するエンティティに対するアクセスルールなし  
 アクセス結果: ✖ アクセスが存在  
 テストタイプ: デバイス[main FW]

ネットワークインタ main FW (VPN)  
 ソース: int15 (内部サーバ)  
 宛先: VPN (パートナー)  
 サービス: 任意

APR 経路: Public Policy/内部サーバ  
 アクセス/内部サーバ~パートナー/アクセスのブロック  
 追加日時: 2007/02/26 15:28:17 JST

説明: デバイスmain FWで、ソース int15 (内部サーバ)と宛先VPN (パートナー)の間にアクセスが見つかりました。  
 APR では、任意のサービスのソースと宛先の間でアクセスを使用できないように指定されています。  
 次の IP アドレス と ポート が宛先にアクセスできます:  
 928973566 IP アドレス:  
 200.160.1.0-200.160.2.0  
 200.160.2.2-200.160.3.0  
 200.160.3.2-200.160.3.255  
 200.161.0.0-255.255.255.255  
  
 197119 ポート:  
 0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN,...)  
 1-65535 (UDP)  
 1-65535 (TCP)  
 0-65535 (RPC)  
 0-255 (IGMP)  
 0-255 (ICMP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (VPN)	200.160.1.0-200.160.2.0
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (VPN)	200.160.2.2-200.160.3.0
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (VPN)	200.160.3.2-200.160.3.255
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (VPN)	200.161.0.0-255.255.255.255

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (VPN)	200.160.1.0-200.160.2.0	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...
main FW (VPN)	200.160.2.2-200.160.3.0	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...
main FW (VPN)	200.160.3.2-200.160.3.255	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...
main FW (VPN)	200.161.0.0-255.255.255.255	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...

**M** 違反 708: int18 (パートナー) -> int2809 (DMZ)

APR: **アクセス制限 - 宛先**

パートナーゾーンとDMZゾーン間のアクセスは、宛先 IP が50個という制限を越えてはなりません。ネットワーク設計のベストプラクティスとして、アクセス制御をネットワークに適用することをお勧めします。この方針に従えば、宛先レベルのアクセス制御が確実に実現され、指定したIPアドレスのみにアクセスが許可されることになります。

**タイプ:** 潜在的なエンティティに対するアクセスルール制限

**アクセス結果:** ✖ アクセス制限を超えました

**テストタイプ:** デバイス[main FW]

**ネットワークインタ** main FW (int2809)

**ソース:** int18 (パートナー)

**宛先:** int2809 (DMZ)

**サービス:** 任意

**宛先 IP に対する制限:** <=50 宛先 IP アドレス

**APR 経路:** Public Policy/パートナーアクセス/パートナー ~ DMZ/アクセス制限 - 宛先

**追加日時:** 2007/02/17 19:48:32 JST

**説明:** デバイスmain FWで、宛先int2809 (DMZ)にアクセスできる IP アドレス数が多すぎます。APR では、50を超える宛先 IP アドレスが 任意のサービスにアクセスできないように制限されています。次の IP アドレスが、アクセスできる IP アドレスの数を超過しています:

**➡️ アクセス可能なターゲット**

指定された制限よりも多くの IP アドレスに到達できるポート範囲

ポート範囲	IP アドレスの数	IP 範囲
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...)	256	192.170.33.0-192.170.33.255
0-255 (ICMP)	256	192.170.33.0-192.170.33.255
0-255 (IGMP)	256	192.170.33.0-192.170.33.255
1-134 (TCP)	256	192.170.33.0-192.170.33.255
135 (TCP)	512	192.170.33.0-192.170.33.255, 192.170.36.0-192.170.36.255
136-442 (TCP)	256	192.170.33.0-192.170.33.255
443 (TCP)	512	192.170.33.0-192.170.33.255, 192.170.36.0-192.170.36.255
444-65535 (TCP)	256	192.170.33.0-192.170.33.255
1-65535 (UDP)	256	192.170.33.0-192.170.33.255
0-65535 (RPC)	256	192.170.33.0-192.170.33.255

**M** 違反 200: int2809 (DMZ) -> int15 (内部サーバ)

APR: **アクセス制限 - 宛先**

DMZゾーンと内部サーバ  
ゾーン間のアクセスは、すべてのサービスの宛先IPが50個という制限を越えてはなりません。  
ネットワーク設計のベスト  
プラクティスとして、アクセス制御をネットワークに適用することをお勧めします。この方針  
に従えば、宛先レベルのアクセス制御が確実に実現され、指定したIPアドレスのみにアクセスが  
許可されることになります。

タイプ: 潜在的なエンティティに対するアクセスルール制限

アクセス結果: ✖ アクセス制限を超えました

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int15 )

ソース: int2809 (DMZ)

宛先: int15 (内部サーバ)

サービス: 任意

宛先 IP に対する制限: <=50 宛先 IP アドレス

APR 経路: Public Policy/DMZアクセス/DMZ ~ 内部サーバ/アクセス制限 - 宛先

追加日時: 2007/02/06 20:57:23 JST

説明: デバイスマイン FWで、宛先int15 (内部サーバ)にアクセスできる IP  
アドレス数が多すぎます。  
APR では、50を超える宛先 IP アドレス が 任意のサービス  
にアクセスできないように制限されています。  
次の IP アドレス が、アクセスできる IP アドレスの数を超過しています:

**⇒** アクセス可能なターゲット

指定された制限よりも多くの IP アドレスに到達できるポート範囲

ポート範囲	IP アドレスの数	IP 範囲
21 (TCP)	768	192.170.17.0-192.170.19.255
23 (TCP)	768	192.170.17.0-192.170.19.255
80 (TCP)	256	192.170.21.0-192.170.21.255
135 (TCP)	256	192.170.21.0-192.170.21.255
8500 (TCP)	256	192.170.27.0-192.170.27.255
135 (UDP)	256	192.170.21.0-192.170.21.255

**M** 違反 94: Internet (外部) -> int15 (内部サーバ)

APR: **アクセスのブロック**

外部ゾーンと内部サーバ  
ゾーン間のアクセスは、すべてのサービスについてブロックする必要があります。ネットワーク設計のベスト プラクティスとして、同じセキュリティレベルのネットワーク間のアクセスを制限することをお勧めします。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int15 )

ソース: Internet (外部)

宛先: int15 (内部サーバ)

サービス: 任意

APR 経路: Public Policy/外部アクセス/外部 ~ 内部サーバ/アクセスのブロック

追加日時: 2007/02/06 20:57:21 JST

説明: デバイスmain FWで、ソース Internet (外部)と宛先int15 (内部サーバ)の間にアクセスが見つかりました。  
APR では、任意のサービスのソースと宛先の間でアクセスを使用できないように指定されています。  
次の IP アドレス と ポート が宛先にアクセスできます:  
768 IP アドレス:  
192.170.17.0-192.170.19.255

2 ポート:  
21 (TCP)  
23 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
21 (TCP), 23 (TCP)	main FW (int15 )	192.170.17.0-192.170.19.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int15 )	192.170.17.0-192.170.19.255	21 (TCP), 23 (TCP)

**M** 違反 717: VPN (パートナー) -> int2809 (DMZ)  
 APR: **アクセス制限 - サービス**

パートナーゾーンとDMZゾーン間のアクセスは、宛先ポートが50個という制限を越えてはなりません。ネットワーク設計のベストプラクティスとして、アクセス制御をネットワークに適用することをお勧めします。この方針に従えば、ポートレベルのアクセス制御が確実に実現され、指定したポートのみにアクセスが許可されることとなります。

**タイプ:** 潜在的なエンティティに対するアクセスルール制限  
**アクセス結果:** ✖ アクセス制限を超えました  
**テストタイプ:** デバイス[main FW]

**ネットワークインタ** main FW (int2809 )  
**ソース:** VPN (パートナー)  
**宛先:** int2809 (DMZ)  
**サービス:** 任意

**宛先ポートに対する制限:** <=50 宛先ポート

**APR 経路:** Public Policy/パートナーアクセス/パートナー ~ DMZ/アクセス制限 - サービス  
**追加日時:** 2007/02/17 19:48:30 JST

**説明:** デバイスマain FWで、宛先int2809 (DMZ)にアクセスできる宛先ポートが多すぎます。APR では、50を超える宛先ポートが、宛先の各 IP アドレスにアクセスできないように制限されています。次の IP アドレスが、アクセスできる宛先ポートの数を超えています: 192.170.33.0-192.170.33.255 - 197119 宛先ポートでアクセス可能です

**⇒⇒ アクセス可能なターゲット**

指定された制限よりも多くのポートから到達できる IP 範囲

IP 範囲	ポート数	ポート範囲
main FW (int2809 ) {Addresses Behind:192.170.1.96-192.170.1.111,192.170.33.0-192.170.36.255}	197,119	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...

**M** 違反 707: int15 (内部サーバ) -> int18 (パートナー)

APR: **アクセスのブロック**

内部サーバゾーンとパートナーゾーン間のアクセスは、すべてのサービスについてブロックする必要があります。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int18)

ソース: int15 (内部サーバ)

宛先: int18 (パートナー)

サービス: 任意

APR 経路: Public Policy/内部サーバ  
アクセス/内部サーバ~パートナー/アクセスのブロック

追加日時: 2007/02/26 15:28:17 JST

説明: デバイスmain FWで、ソース int15 (内部サーバ)と宛先int18 (パートナー)の間にアクセスが見つかりました。  
APR では、任意のサービスのソースと宛先の間でアクセスを使用できないように指定されています。

次の IP アドレス と ポート が宛先にアクセスできます:

255 IP アドレス:

200.160.2.0  
200.160.2.2-200.160.2.255

197119 ポート:

0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN,...)

1-65535 (UDP)

1-65535 (TCP)

0-65535 (RPC)

0-255 (IGMP)

0-255 (ICMP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (int18)	200.160.2.0
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (int18)	200.160.2.2-200.160.2.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int18)	200.160.2.0	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...
main FW (int18)	200.160.2.2-200.160.2.255	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...

**M** 違反 7: Internet (外部) -> int2809 (DMZ)

APR: DNSアクセスの制限

外部ゾーンとDMZゾーン間のDNSアクセスは、宛先IPが5個という制限を越えてはなりません。一般的なDMZ環境では、少数のDNSサーバを使用すべきです。このルールに違反すると、ファイアウォールが正しく構成されず、不適切なDNSクエリーアクセスまたはDNSゾーン転送アクセスにDMZがさらされる可能性があります。

タイプ: 潜在的なエンティティに対するアクセスルール制限

アクセス結果: ✖ アクセス制限を超えました

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: Internet (外部)

宛先: int2809 (DMZ)

サービス: [53/UDP] - domain\_u, [53/TCP] - domain\_t

宛先 IP に対する制限: <=5 宛先 IP アドレス

APR 経路: Public Policy/外部アクセス/外部 ~ DMZ/DNSアクセスの制限

追加日時: 2007/02/06 20:57:21 JST

説明: デバイスmain FWで、宛先int2809 (DMZ)にアクセスできる IP アドレス数が多すぎます。APR では、5を超える宛先 IP アドレスが各サービス: [53/UDP] - domain\_u, [53/TCP] - domain\_t にアクセスできないように制限されています。次の IP アドレスが、アクセスできる IP アドレスの数を超えています:

**⇒** アクセス可能なターゲット

指定された制限よりも多くの IP アドレスに到達できるポート範囲

ポート範囲	IP アドレスの数	IP 範囲
53 (TCP)	256	192.170.33.0-192.170.33.255
53 (UDP)	256	192.170.33.0-192.170.33.255

**M** 違反 694: int18 (パートナー) -> int15 (内部サーバ)

APR: **アクセス制限 - 宛先**

パートナーゾーンと内部サーバゾーン間のアクセスは、宛先 IP が50個という制限を越えてはなりません。ネットワーク設計のベストプラクティスとして、アクセス制御をネットワークに適用することをお勧めします。この方針に従えば、宛先レベルのアクセス制御が確実に実現され、指定したIPアドレスのみにアクセスが許可されることになります。

タイプ: 潜在的なエンティティに対するアクセスルール制限

アクセス結果: ✖ アクセス制限を超えました

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int15)

ソース: int18 (パートナー)

宛先: int15 (内部サーバ)

サービス: 任意

宛先 IP に対する制限: <=50 宛先 IP アドレス

APR 経路: Public Policy/パートナーアクセス/パートナー~内部サーバ/アクセス制限 - 宛先

追加日時: 2007/02/17 19:48:32 JST

説明: デバイスmain FWで、宛先int15 (内部サーバ)にアクセスできる IP アドレス数が多すぎます。APR では、50を超える宛先 IP アドレス が 任意のサービス にアクセスできないように制限されています。次の IP アドレス が、アクセスできる IP アドレスの数を超過しています:

**⇒** アクセス可能なターゲット

指定された制限よりも多くの IP アドレスに到達できるポート範囲

ポート範囲	IP アドレスの数	IP 範囲
21 (TCP)	768	192.170.17.0-192.170.19.255
23 (TCP)	768	192.170.17.0-192.170.19.255

**M** 違反 243: int15 (内部サーバ) -> int2809 (DMZ)  
 APR: X-Windowsのブロック

内部サーバ  
 ゾーンとDMZゾーン間のX-Windowsサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワーク  
 ゾーン間におけるX-Windowsサービスは使用すべきではありません。X-Windowsサービスを使用するとリモート管理が可能になるため、信頼できるソースからのX-Windowsサービスのみを許可してください。

タイプ: 潜在するエンティティに対するアクセスルールなし  
 アクセス結果: ✖ アクセスが存在  
 テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809 )  
 ソース: int15 (内部サーバ)  
 宛先: int2809 (DMZ)  
 サービス: 6000-6255/TCP

APR 経路: Public Policy/内部サーバ アクセス/内部サーバ ~ DMZ/X-Windowsのブロック  
 追加日時: 2007/02/06 20:57:22 JST

説明: デバイスmain FWで、ソース int15 (内部サーバ)と宛先int2809 (DMZ)の間にアクセスが見つかりました。  
 APR では、サービス 6000-6255/TCP のソースと宛先の間でアクセスを使用できないように指定されています。  
 次の IP アドレス と ポート が宛先にアクセスできます:  
 1040 IP アドレス:  
 192.170.1.96-192.170.1.111  
 192.170.33.0-192.170.36.255  
  
 256 ポート:  
 6000-6255 (TCP)

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
6000-6255 (TCP)	main FW (int2809 )	192.170.1.96-192.170.1.111
6000-6255 (TCP)	main FW (int2809 )	192.170.33.0-192.170.36.255

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809 )	192.170.1.96-192.170.1.111	6000-6255 (TCP)
main FW (int2809 )	192.170.33.0-192.170.36.255	6000-6255 (TCP)

**M** 違反 236: int15 (内部サーバ) -> int2809 (DMZ)

APR: RPCとNFSのブロック

内部サーバ

ゾーンとDMZゾーン間のRPCサービスとNFSサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるRPCサービスとNFSサービスは使用すべきではありません。その理由は、これらのサービスが数多くの脆弱性を持つことが分かっているためです。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int15 (内部サーバ)

宛先: int2809 (DMZ)

サービス: [111/TCP,111/UDP] - sunrpc, [2049/TCP,2049/UDP,100003/RPC] - nfs, nlockmgr [100021/RPC,4045/TCP,4045/UDP]

APR 経路: Public Policy/内部サーバ アクセス/内部サーバ ~ DMZ/RPCとNFSのブロック

追加日時: 2007/02/06 20:57:22 JST

説明:

デバイスmain FWで、ソース int15 (内部サーバ)と宛先int2809 (DMZ)の間にアクセスが見つかりました。  
 APR では、任意のサービス:[111/TCP, 111/UDP] - sunrpc, [2049/TCP, 2049/UDP, 100003/RPC] - nfs, nlockmgr [100021/RPC, 4045/TCP, 4045/UDP] のソースと宛先の間でアクセスを使用できないように指定されています。  
 次の IP アドレス と ポート が宛先にアクセスできます:  
 1040 IP アドレス:  
 192.170.1.96-192.170.1.111  
 192.170.33.0-192.170.36.255

6 ポート:  
 4045 (TCP)  
 4045 (UDP)  
 111 (UDP)  
 111 (TCP)  
 2049 (UDP)  
 2049 (TCP)

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
111 (TCP), 2049 (TCP), 4045 (TCP), 111 (UDP), 2049 (UDP), 4045 (UDP)	main FW (int2809)	192.170.1.96-192.170.1.111
111 (TCP), 2049 (TCP), 4045 (TCP), 111 (UDP), 2049 (UDP), 4045 (UDP)	main FW (int2809)	192.170.33.0-192.170.36.255

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.1.96-192.170.1.111	111 (TCP), 2049 (TCP), 4045 (TCP), 111 (UDP), 2049 (UDP), 4045 (UDP)
main FW (int2809)	192.170.33.0-192.170.36.255	111 (TCP), 2049 (TCP), 4045 (TCP), 111 (UDP), 2049 (UDP), 4045 (UDP)

**M** 違反 5: Internet (外部) -> int2809 (DMZ)

APR: HTTPアクセスの制限

外部ゾーンとDMZゾーン間のHTTPおよびHTTPSアクセスは、宛先IPが50個という制限を越えてはなりません。一般的なDMZ環境では、Webサーバの個数を制限する必要があります。このルールに違反すると、ファイアウォールが正しく構成されず、不適切なHTTP/SアクセスにDMZがさらされる可能性があります。

タイプ: 潜在的なエンティティに対するアクセスルール制限

アクセス結果: ✖ アクセス制限を超えました

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: Internet (外部)

宛先: int2809 (DMZ)

サービス: [443/TCP,8443/TCP] - https, [80/TCP,8080/TCP] - http

宛先 IP に対する制限: <=50 宛先 IP アドレス

APR 経路: Public Policy/外部アクセス/外部 ~ DMZ/HTTPアクセスの制限

追加日時: 2007/02/06 20:57:21 JST

説明: デバイスmain FWで、宛先int2809 (DMZ)にアクセスできる IP アドレス数が多すぎます。  
APR では、50を超える宛先 IP アドレス が 各サービス: [443/TCP, 8443/TCP] - https, [80/TCP, 8080/TCP] - http にアクセスできないように制限されています。  
次の IP アドレス が、アクセスできる IP アドレスの数を超過しています:

**⇒** アクセス可能なターゲット

指定された制限よりも多くの IP アドレスに到達できるポート範囲

ポート範囲	IP アドレスの数	IP 範囲
80 (TCP)	256	192.170.33.0-192.170.33.255
443 (TCP)	256	192.170.33.0-192.170.33.255

**M** 違反 271: int15 (内部サーバ) -> int2809 (DMZ)

APR: ICMP 応答メッセージのブロック

内部サーバ

ゾーンとDMZゾーン間のICMP応答メッセージはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワーク

ゾーン間におけるICMP応答メッセージ(Echo Replyなど)は使用すべきではありません。ICMP応答メッセージは、サイバー攻撃の基本であるネットワーク偵察行為の一部として使用される可能性があります。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int15 (内部サーバ)

宛先: int2809 (DMZ)

サービス: 0/ICMP, 3/ICMP, 4/ICMP, 11/ICMP, 12/ICMP

APR 経路: Public Policy/内部サーバ  
アクセス/内部サーバ ~ DMZ/ICMP 応答メッセージのブロック

追加日時: 2007/02/06 20:57:22 JST

説明: デバイス main FW で、ソース int15 (内部サーバ) と宛先 int2809 (DMZ) の間にアクセスが見つかりました。APR では、任意のサービス: 0/ICMP, 3/ICMP, 4/ICMP, 11/ICMP, 12/ICMP のソースと宛先の間でアクセスを使用できないように指定されています。次の IP アドレス と ポート が宛先にアクセスできます:

1040 IP アドレス:  
192.170.1.96-192.170.1.111  
192.170.33.0-192.170.36.255

5 ポート:  
11-12 (ICMP)  
3-4 (ICMP)  
0 (ICMP)

**➡** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
0 (ICMP), 3-4 (ICMP), 11-12 (ICMP)	main FW (int2809)	192.170.1.96-192.170.1.111
0 (ICMP), 3-4 (ICMP), 11-12 (ICMP)	main FW (int2809)	192.170.33.0-192.170.36.255

**➡** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.1.96-192.170.1.111	0 (ICMP), 3-4 (ICMP), 11-12 (ICMP)
main FW (int2809)	192.170.33.0-192.170.36.255	0 (ICMP), 3-4 (ICMP), 11-12 (ICMP)

**M** 違反 729: int2809 (DMZ) -> VPN (パートナー)

APR: **アクセスのブロック**

DMZゾーンとパートナーゾーン間のアクセスは、すべてのサービスについてブロックする必要があります。

タイプ: 潜在するエンティティに対するアクセスルールなし  
 アクセス結果: **✖** アクセスが存在  
 テストタイプ: デバイス[main FW]

ネットワークインタ main FW (VPN)

ソース: int2809 (DMZ)  
 宛先: VPN (パートナー)  
 サービス: 任意

APR 経路: Public Policy/DMZアクセス/DMZ ~ パートナー/アクセスのブロック

追加日時: 2007/02/26 15:28:18 JST

説明: デバイスmain FWで、ソース int2809 (DMZ)と宛先VPN (パートナー)の間にアクセスが見つかりました。APR では、任意のサービスのソースと宛先の間でアクセスを使用できないように指定されています。次の IP アドレス と ポート が宛先にアクセスできます:  
 511 IP アドレス:  
 200.160.1.0-200.160.2.0  
 200.160.2.2-200.160.2.255  
 1 ポート:  
 69 (UDP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
69 (UDP)	main FW (VPN)	200.160.1.0-200.160.2.0
69 (UDP)	main FW (VPN)	200.160.2.2-200.160.2.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (VPN)	200.160.1.0-200.160.2.0	69 (UDP)
main FW (VPN)	200.160.2.2-200.160.2.255	69 (UDP)

**M** 違反 720: VPN (パートナー) -> int15 (内部サーバ)

APR: **アクセス制限 - 宛先**

パートナーゾーンと内部サーバゾーン間のアクセスは、宛先 IP が50個という制限を越えてはなりません。ネットワーク設計のベストプラクティスとして、アクセス制御をネットワークに適用することをお勧めします。この方針に従えば、宛先レベルのアクセス制御が確実に実現され、指定したIPアドレスのみにアクセスが許可されることになります。

タイプ: 潜在的なエンティティに対するアクセスルール制限

アクセス結果: ✖ アクセス制限を超えました

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int15)

ソース: VPN (パートナー)

宛先: int15 (内部サーバ)

サービス: 任意

宛先 IP に対する制限: <=50 宛先 IP アドレス

APR 経路: Public Policy/パートナーアクセス/パートナー~内部サーバ/アクセス制限 - 宛先

追加日時: 2007/02/17 19:48:30 JST

説明: デバイスmain FWで、宛先int15 (内部サーバ)にアクセスできる IP アドレス数が多すぎます。APR では、50を超える宛先 IP アドレス が 任意のサービス にアクセスできないように制限されています。次の IP アドレス が、アクセスできる IP アドレスの数を超えています:

**⇒** アクセス可能なターゲット

指定された制限よりも多くの IP アドレスに到達できるポート範囲

ポート範囲	IP アドレスの数	IP 範囲
21 (TCP)	768	192.170.17.0-192.170.19.255
23 (TCP)	768	192.170.17.0-192.170.19.255

**M** 違反 250: int15 (内部サーバ) -> int2809 (DMZ)

APR: **スモール サービスのブロック**

内部サーバゾーンとDMZゾーン間のスモールサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるスモールサービスグループは使用すべきではありません。その理由は、これらのサービスが数多くの脆弱性を持つことが分かっているためです。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int15 (内部サーバ)

宛先: int2809 (DMZ)

サービス: [37/TCP,37/UDP] - time, 1-20/TCP, 1-20/UDP

APR 経路: Public Policy/内部サーバ アクセス/内部サーバ~DMZ/スモールサービスのブロック

追加日時: 2007/02/06 20:57:22 JST

説明: デバイスmain FWで、ソース int15 (内部サーバ)と宛先int2809 (DMZ)の間にアクセスが見つかりました。  
APR では、任意のサービス: [37/TCP, 37/UDP] - time, 1-20/TCP, 1-20/UDP のソースと宛先の間でアクセスを使用できないように指定されています。  
次の IP アドレス と ポート が宛先にアクセスできます:  
1040 IP アドレス:  
192.170.1.96-192.170.1.111  
192.170.33.0-192.170.36.255

42 ポート:  
1-20 (UDP)  
1-20 (TCP)  
37 (UDP)  
37 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
1-20 (TCP), 37 (TCP), 1-20 (UDP), 37 (UDP)	main FW (int2809)	192.170.1.96-192.170.1.111
1-20 (TCP), 37 (TCP), 1-20 (UDP), 37 (UDP)	main FW (int2809)	192.170.33.0-192.170.36.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809)	192.170.1.96-192.170.1.111	1-20 (TCP), 37 (TCP), 1-20 (UDP), 37 (UDP)
main FW (int2809)	192.170.33.0-192.170.36.255	1-20 (TCP), 37 (TCP), 1-20 (UDP), 37 (UDP)

**M** 違反 264: int15 (内部サーバ) -> int2809 (DMZ)

APR: トロイ/ワーム ポートのブロック

内部サーバゾーンとDMZゾーン間のトロイ/ワーム  
ポートはブロックする必要があります。NIST公開仕様800-41によれば、このグループのポートはワ  
ームとトロイによって使用されることが分かっているため、ブロックする必要があります。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int15 (内部サーバ)

宛先: int2809 (DMZ)

サービス: '4553' [21227/TCP,21317/TCP], accessremotepc [34012/TCP], agent\_40421  
[30/TCP,40421/TCP], anig [5190/TCP], aok [8961/TCP], aol-admin  
[30029/TCP], asylum [23432/TCP], attackftp [666/TCP], Backdoor.Akak  
[4321/TCP], Backdoor.Emcommander [31337/TCP], Backdoor.Hale  
[6351/TCP,5555/TCP,48522/TCP], BackOrifice [31337/UDP], bagel  
[6777/TCP], beagle.b [8866/TCP], beagle.e [2745/TCP], beagle.j [2745/TCP],  
beagle.m [2556/TCP], beagle.u [4751/TCP], beagle.w [2535/TCP], beagle.x  
[2535/TCP], biggluck [34324/TCP], bind-shell [33270/TCP], bionet [12349/TCP],  
blaster [4444/TCP], blazer5 [5000/TCP], bo2k [54320/TCP,54321/UDP], bofra  
[1639/TCP,1640/TCP], bolgi [5732/TCP], bugbear [36794/TCP], bugs  
[2115/TCP], bunker\_hill [61348/TCP,61603/TCP,63485/TCP], Cdk  
[15858/TCP,79/TCP], chupacabra [13473/TCP,20203/TCP], coma  
[10607/TCP], connection [8720/TCP,60411/TCP,60412/TCP], crazzynet  
[17499/TCP,17500/TCP], dabber  
[9898/TCP,9899/TCP,9900/TCP,9901/TCP,9999/TCP], dagger  
[2589/TCP,1386/TCP], death [2/TCP], deepthroat  
[2140/UDP,3150/UDP,6670/TCP,6771/TCP,60000/TCP], deltasource  
[6883/TCP], Dipnet [11768/TCP,15118/TCP], doom\_backdoor [10167/UDP],  
drat [48/TCP,50/TCP], event-horizon [4488/TCP], evilftp [12346/TCP], Explet  
[1250/TCP], fluxay [10/TCP], forced-entry [1025/TCP,9999/TCP], freak88  
[7001/UDP,31337/UDP], frenzy [1257/TCP], Gaobot Backdoor  
[1749/TCP,63809/TCP], Gaobot Backward [22226/TCP,13659/TCP],  
gatecrasher [6969/TCP], girlfriend [21554/TCP], glacier [7626/TCP],  
globe\_backdoor [28876/TCP], hackatack [31785/TCP,31789/UDP,31791/UDP],  
helemoo [28876/TCP], host-control [11051/TCP], Huayu [887/TCP], HVL-RAT  
[1095/TCP,1097/TCP,1098/TCP,1099/TCP], incommand [9400/TCP], ingreslock  
[1524/TCP,1524/UDP], jade [1024/TCP,65421/TCP], Janx [5533/TCP], Kibuv  
[5300/TCP,420/TCP], Kibuv-ftp [9604/TCP,7955/TCP], Kipis.L [5311/TCP],  
knooth.e [11040/TCP], kuang2 [17300/TCP], lateda [9999/TCP], Linux OSF  
[29369/TCP,29369/UDP], Linux.Plupii [7222/UDP], lion  
[6008/TCP,33567/TCP,33568/TCP], litmus [30005/TCP], lovgate  
[10168/TCP,6000/TCP], mantis [37237/TCP], matrix  
[1269/TCP,1025/UDP,1025/TCP], millenium [20000/TCP,20001/TCP],  
mstream\_agent [10498/UDP,7983/UDP], mstream\_handler  
[6723/TCP,15104/TCP,12754/TCP], mydoom  
[3127/TCP,3198/TCP,1034/TCP,10080/TCP,1042/TCP,1080/TCP], MySQL Bot  
[2301/TCP,2304/TCP], Mytob.AI [10087/TCP], Mytob.AJ [61137/TCP],  
Mytob.AR [10089/TCP], Mytob.BB Backdoor [10155/TCP], Mytob.BB Backward  
[10487/TCP], Mytob.BH [12187/TCP], Mytob.BL [10085/TCP], Mytob.CM  
[10082/TCP], Mytob.FX [10099/TCP], NetBus  
[12345/TCP,12346/TCP,20034/TCP], netdemon [15000/TCP], netmonitor  
[7300/TCP,7301/TCP,7306/TCP,7307/TCP,7308/TCP], Netsky  
[5556/TCP,5557/TCP], netsphere [30100/TCP,30102/TCP], netspy  
[1033/TCP], phatbot [4387/TCP], ... (71 - 追加サービス)

APR 経路: Public Policy/内部サーバ アクセス/内部サーバ~DMZ/トロイ/ワーム  
ポートのブロック

追加日時: 2007/02/06 20:57:22 JST

説明:

デバイスmain FWで、ソース int15 (内部サーバ)と宛先int2809 (DMZ)の間にアクセスが見つかりました。  
 APR では、任意のサービス:'4553' [21227/TCP, 21317/TCP], accessremotepc [34012/TCP], agent\_40421 [30/TCP, 40421/TCP], anig [5190/TCP], aok [8961/TCP], aol-admin [30029/TCP], asylum [23432/TCP], attackftp [666/TCP], 258 以上のソースと宛先の間でアクセスを使用できないように指定されています。  
 次の IP アドレス と ポート が宛先にアクセスできます:  
 1040 IP アドレス:  
 192.170.1.96-192.170.1.111  
 192.170.33.0-192.170.36.255

246 ポート:  
 30100 (TCP)  
 6868 (TCP)  
 3150 (UDP)  
 1 (UDP)  
 21317 (TCP)  
 11768 (TCP)  
 65000 (TCP)  
 31789 (UDP)  
 2140 (UDP)  
 29369 (TCP)  
 197 以上

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
2 (TCP), 8 (TCP), 10 (TCP), 30 (TCP), 48 (TCP), 50 (TCP), 79 (TCP), 420-421 (TCP), 531 (TCP), 559 ...	main FW (int2809 )	192.170.1.96-192.170.1.111
2 (TCP), 8 (TCP), 10 (TCP), 30 (TCP), 48 (TCP), 50 (TCP), 79 (TCP), 420-421 (TCP), 531 (TCP), 559 ...	main FW (int2809 )	192.170.33.0-192.170.36.255

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809 )	192.170.1.96-192.170.1.111	2 (TCP), 8 (TCP), 10 (TCP), 30 (TCP), 48 (TCP), 50 (TCP), 79 (TCP), 420-421 (TCP), 531 (TCP), 559 ...
main FW (int2809 )	192.170.33.0-192.170.36.255	2 (TCP), 8 (TCP), 10 (TCP), 30 (TCP), 48 (TCP), 50 (TCP), 79 (TCP), 420-421 (TCP), 531 (TCP), 559 ...

**M** 違反 229: int15 (内部サーバ) -> int2809 (DMZ)

APR: **ログイン サービスのブロック**

内部サーバゾーンとDMZゾーン間のログインサービスはブロックする必要があります。NIST公開仕様800-41によれば、セキュリティレベルが異なるネットワークゾーン間におけるログインサービス(Telnet、SSHなど)は使用すべきではありません。ログインサービスを使用するとリモート管理が可能になるため、信頼できるソースからのログインサービスのみを許可してください。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int15 (内部サーバ)

宛先: int2809 (DMZ)

サービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP,129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shell

APR 経路: Public Policy/内部サーバ アクセス/内部サーバ~DMZ/ログインサービスのブロック

追加日時: 2007/02/06 20:57:22 JST

説明: デバイスmain FWで、ソース int15 (内部サーバ)と宛先int2809 (DMZ)の間にアクセスが見つかりました。APR では、任意のサービス: [23/TCP] - telnet, [22/TCP] - ssh, [129/TCP, 129/UDP] - pwdgen, [512/TCP] - exec, [513/TCP] - rlogin, [514/TCP] - shell のソースと宛先の間でアクセスを使用できないように指定されています。次の IP アドレス と ポート が宛先にアクセスできます:

1040 IP アドレス:  
192.170.1.96-192.170.1.111  
192.170.33.0-192.170.36.255

7 ポート:  
129 (UDP)  
22-23 (TCP)  
512-514 (TCP)  
129 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
22-23 (TCP), 129 (TCP), 512-514 (TCP), 129 (UDP)	main FW (int2809 )	192.170.1.96-192.170.1.111
22-23 (TCP), 129 (TCP), 512-514 (TCP), 129 (UDP)	main FW (int2809 )	192.170.33.0-192.170.36.255

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int2809 )	192.170.1.96-192.170.1.111	22-23 (TCP), 129 (TCP), 512-514 (TCP), 129 (UDP)
main FW (int2809 )	192.170.33.0-192.170.36.255	22-23 (TCP), 129 (TCP), 512-514 (TCP), 129 (UDP)

**M** 違反 227: int15 (内部サーバ) -> Internet (外部)  
 APR: アクセスのブロック

内部サーバ  
 ゾーンと外部ゾーン間のアクセスは、すべてのサービスについてブロックする必要があります。  
 ネットワーク設計のベストプラクティスとして、同じセキュリティレベルのネットワーク間のアクセスを制限することをお勧めします。

タイプ: 潜在するエンティティに対するアクセスルールなし  
 アクセス結果: ✖ アクセスが存在  
 テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int19)

ソース: int15 (内部サーバ)  
 宛先: Internet (外部)  
 サービス: 任意

APR 経路: Public Policy/内部サーバ アクセス/内部サーバ~外部/アクセスのブロック

追加日時: 2007/02/06 20:57:22 JST

説明: デバイスmain FWで、ソース int15 (内部サーバ)と宛先Internet (外部)の間にアクセスが見つかりました。  
 APR では、任意のサービスのソースと宛先の間でアクセスを使用できないように指定されています。  
 次の IP アドレスとポートが宛先にアクセスできます:  
 3365989760 IP アドレス:  
 0.0.0.0-192.169.0.255  
 192.169.1.16-192.170.0.255  
 192.170.1.112-192.170.7.255  
 192.170.9.0-192.170.15.255  
 192.170.20.0-192.170.20.255  
 192.170.24.0-192.170.24.255  
 192.170.28.0-192.170.32.255  
 192.170.37.0-200.160.0.255  
 200.160.4.0-200.160.255.255  
  
 197119 ポート:  
 0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN,...)  
 1-65535 (UDP)  
 1-65535 (TCP)  
 0-65535 (RPC)  
 0-255 (IGMP)  
 0-255 (ICMP)

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (int19)	192.169.1.16-192.170.0.255
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (int19)	192.170.1.112-192.170.7.255

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (int19 )	192.170.9.0-192.170.15.255
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (int19 )	192.170.20.0-192.170.20.255
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (int19 )	192.170.24.0-192.170.24.255
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (int19 )	192.170.28.0-192.170.32.255
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (int19 )	192.170.37.0-200.160.0.255
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (int19 )	200.160.4.0-200.160.255.255
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...	main FW (int19 )	0.0.0.0-192.169.0.255

➡️ アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int19 )	192.169.1.16-192.170.0.255	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...
main FW (int19 )	192.170.1.112-192.170.7.255	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...
main FW (int19 )	192.170.9.0-192.170.15.255	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...
main FW (int19 )	192.170.20.0-192.170.20.255	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...
main FW (int19 )	192.170.24.0-192.170.24.255	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...
main FW (int19 )	192.170.28.0-192.170.32.255	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...
main FW (int19 )	192.170.37.0-200.160.0.255	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...


ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int19 )	200.160.4.0-200.160.255.255	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...
main FW (int19 )	0.0.0.0-192.169.0.255	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...

**M** 違反 691: int18 (パートナー) -> int2809 (DMZ)

APR: **アクセス制限 - サービス**

パートナーゾーンとDMZゾーン間のアクセスは、宛先ポートが50個という制限を越えてはなりません。ネットワーク設計のベストプラクティスとして、アクセス制御をネットワークに適用することをお勧めします。この方針に従えば、ポートレベルのアクセス制御が確実に実現され、指定したポートのみにアクセスが許可されることとなります。

**タイプ:** 潜在的なエンティティに対するアクセスルール制限

**アクセス結果:**  アクセス制限を超えました

**テストタイプ:** デバイス[main FW]

**ネットワークインタ** main FW (int2809 )

**ソース:** int18 (パートナー)

**宛先:** int2809 (DMZ)

**サービス:** 任意

**宛先ポートに対する制限:** <=50 宛先ポート

**APR 経路:** Public Policy/パートナーアクセス/パートナー ~ DMZ/アクセス制限 - サービス

**追加日時:** 2007/02/17 19:48:32 JST

**説明:** デバイスmain FWで、宛先int2809 (DMZ)にアクセスできる宛先ポートが多すぎます。APR では、50を超える宛先ポートが、宛先の各 IP アドレスにアクセスできないように制限されています。次の IP アドレスが、アクセスできる宛先ポートの数を超過しています: 192.170.33.0-192.170.33.255 - 197119 宛先ポートでアクセス可能です

**⇒** アクセス可能なターゲット

指定された制限よりも多くのポートから到達できる IP 範囲

IP 範囲	ポート数	ポート範囲
main FW (int2809 ) {Addresses Behind:192.170.1.96-192.170.1.111,192.170.33.0-192.170.36.255}	197,119	0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...), 0-255 (ICMP), 0-255 (IGMP), 1-65535 (TCP), 1-65535 ...

**M** 違反 278: int15 (内部サーバ) -> int2809 (DMZ)

APR: **アクセス制限 - 宛先**

内部サーバ

ゾーンとDMZゾーン間のアクセスは、すべてのサービスの宛先IPが50個という制限を越えてはなりません。ネットワーク設計のベストプラクティスとして、アクセス制御をネットワークに適用することをお勧めします。この方針に従えば、宛先レベルのアクセス制御が確実に実現され、指定したIPアドレスのみにアクセスが許可されることになります。

タイプ: 潜在的なエンティティに対するアクセスルール制限

アクセス結果: ✖ アクセス制限を超えました

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: int15 (内部サーバ)

宛先: int2809 (DMZ)

サービス: 任意

宛先 IP に対する制限: <=50 宛先 IP アドレス

APR 経路: Public Policy/内部サーバ アクセス/内部サーバ ~ DMZ/アクセス制限 - 宛先

追加日時: 2007/02/06 20:57:22 JST

説明: デバイスmain FWで、宛先int2809 (DMZ)にアクセスできる IP アドレス数が多すぎます。  
APR では、50を超える宛先 IP アドレス が任意のサービスにアクセスできないように制限されています。  
次の IP アドレス が、アクセスできる IP アドレスの数を超過しています:

**⇒** アクセス可能なターゲット

指定された制限よりも多くの IP アドレスに到達できるポート範囲

ポート範囲	IP アドレスの数	IP 範囲
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...)	1,040	192.170.1.96-192.170.1.111, 192.170.33.0-192.170.36.255
0-255 (ICMP)	1,040	192.170.1.96-192.170.1.111, 192.170.33.0-192.170.36.255
0-255 (IGMP)	1,040	192.170.1.96-192.170.1.111, 192.170.33.0-192.170.36.255
1-65535 (TCP)	1,040	192.170.1.96-192.170.1.111, 192.170.33.0-192.170.36.255
1-65535 (UDP)	1,040	192.170.1.96-192.170.1.111, 192.170.33.0-192.170.36.255
0-65535 (RPC)	1,040	192.170.1.96-192.170.1.111, 192.170.33.0-192.170.36.255

**M** 違反 734: VPN (パートナー) -> int2809 (DMZ)

APR: **アクセス制限 - 宛先**

パートナーゾーンとDMZゾーン間のアクセスは、宛先 IP が50個という制限を越えてはなりません。ネットワーク設計のベストプラクティスとして、アクセス制御をネットワークに適用することをお勧めします。この方針に従えば、宛先レベルのアクセス制御が確実に実現され、指定したIPアドレスのみにアクセスが許可されることになります。

タイプ: 潜在的なエンティティに対するアクセスルール制限

アクセス結果: ✖ アクセス制限を超えました

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int2809)

ソース: VPN (パートナー)

宛先: int2809 (DMZ)

サービス: 任意

宛先 IP に対する制限: <=50 宛先 IP アドレス

APR 経路: Public Policy/パートナーアクセス/パートナー ~ DMZ/アクセス制限 - 宛先

追加日時: 2007/02/17 19:48:30 JST

説明: デバイスmain FWで、宛先int2809 (DMZ)にアクセスできる IP アドレス数が多すぎます。  
APR では、50を超える宛先 IP アドレスが 任意のサービスにアクセスできないように制限されています。  
次の IP アドレスが、アクセスできる IP アドレスの数を超過しています:

**⇒** アクセス可能なターゲット

指定された制限よりも多くの IP アドレスに到達できるポート範囲

ポート範囲	IP アドレスの数	IP 範囲
0 (3PC, AH, AN, ARGUS, ARIS, AX25, BBN, ...)	256	192.170.33.0-192.170.33.255
0-255 (ICMP)	256	192.170.33.0-192.170.33.255
0-255 (IGMP)	256	192.170.33.0-192.170.33.255
1-134 (TCP)	256	192.170.33.0-192.170.33.255
135 (TCP)	512	192.170.33.0-192.170.33.255, 192.170.36.0-192.170.36.255
136-442 (TCP)	256	192.170.33.0-192.170.33.255
443 (TCP)	512	192.170.33.0-192.170.33.255, 192.170.36.0-192.170.36.255
444-65535 (TCP)	256	192.170.33.0-192.170.33.255
1-65535 (UDP)	256	192.170.33.0-192.170.33.255
0-65535 (RPC)	256	192.170.33.0-192.170.33.255

**M** 違反 220: int15 (内部サーバ) -> Internet (外部)

APR: VPN アクセスのブロック

内部サーバゾーンと外部ゾーン間の VPN アクセスはブロックする必要があります。このルールに違反すると、不正なアウトバウンド VPN アクセスにさらされる場合があります。

タイプ: 潜在するエンティティに対するアクセスルールなし

アクセス結果: ✖ アクセスが存在

テストタイプ: デバイス[main FW]

ネットワークインタ main FW (int19)

ソース: int15 (内部サーバ)

宛先: Internet (外部)

サービス: isakmp [500/TCP,500/UDP], l2tpd [1701/TCP,1701/UDP], pptp [1723/TCP], Any/ESP, Any/GRE

APR 経路: Public Policy/内部サーバ アクセス/内部サーバ~外部/VPN アクセスのブロック

追加日時: 2007/02/06 20:57:22 JST

説明: デバイスmain FWで、ソース int15 (内部サーバ)と宛先Internet (外部)の間にアクセスが見つかりました。  
APR では、任意のサービス: isakmp [500/TCP, 500/UDP], l2tpd [1701/TCP, 1701/UDP], pptp [1723/TCP], 任意/ESP, 任意/GRE のソースと宛先の間でアクセスを使用できないように指定されています。  
次の IP アドレスとポートが宛先にアクセスできます:  
3365989760 IP アドレス:  
0.0.0.0-192.169.0.255  
192.169.1.16-192.170.0.255  
192.170.1.112-192.170.7.255  
192.170.9.0-192.170.15.255  
192.170.20.0-192.170.20.255  
192.170.24.0-192.170.24.255  
192.170.28.0-192.170.32.255  
192.170.37.0-200.160.0.255  
200.160.4.0-200.160.255.255

7 ポート:  
1723 (UDP)  
1723 (TCP)  
1701 (TCP)  
1701 (UDP)  
0 (ESP, GRE)  
500 (UDP)  
500 (TCP)

**⇒** アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (ポート別にグループ表示)

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)	main FW (int19)	192.169.1.16-192.170.0.255
0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)	main FW (int19)	192.170.1.112-192.170.7.255
0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)	main FW (int19)	192.170.9.0-192.170.15.255

ポート(サービス)	ネットワーク	IP 範囲 (ホスト)
0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)	main FW (int19 )	192.170.20.0-192.170.20.255
0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)	main FW (int19 )	192.170.24.0-192.170.24.255
0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)	main FW (int19 )	192.170.28.0-192.170.32.255
0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)	main FW (int19 )	192.170.37.0-200.160.0.255
0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)	main FW (int19 )	200.160.4.0-200.160.255.255
0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)	main FW (int19 )	0.0.0.0-192.169.0.255

📡 アクセス可能なターゲット

ソースから到達できる IP 範囲とポート範囲 (IP 範囲別にグループ表示)

ネットワーク	IP 範囲 (ホスト)	ポート(サービス)
main FW (int19 )	192.169.1.16-192.170.0.255	0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)
main FW (int19 )	192.170.1.112-192.170.7.255	0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)
main FW (int19 )	192.170.9.0-192.170.15.255	0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)
main FW (int19 )	192.170.20.0-192.170.20.255	0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)
main FW (int19 )	192.170.24.0-192.170.24.255	0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)
main FW (int19 )	192.170.28.0-192.170.32.255	0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)
main FW (int19 )	192.170.37.0-200.160.0.255	0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)
main FW (int19 )	200.160.4.0-200.160.255.255	0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)
main FW (int19 )	0.0.0.0-192.169.0.255	0 (ESP, GRE), 500 (TCP), 1701 (TCP), 1723 (TCP), 500 (UDP), 1701 (UDP), 1723 (UDP)

## 4. レポートプロパティ

次の表にはレポートで選択されたフィルタが表示されます。

Report Type	デバイスコンプライアンス
Generated at	2008/05/27 10:49:35 JST
Model	現状
基本	
詳細レベル	Details
ネットワーク スコープ	main FW [192.169.1.1]
違反パラメータ	
ポリシー スコープ	パブリックポリシー
重要性のしきい値	Any
デバイスパラメータ	
ホスト タイプ	Any
デバイスタイプ	Any
OS	Any
最終計算日時	Any
詳細	
違反のみ表示	Yes
ACL ルールの表示	Yes
表示される最大アクセス結果	50
ロケーションでグループ化	No
サービスの最大数	100
アクセス結果表示	
アクセス ルールなし	by IP Ranges and Ports
フルアクセス ルール	by IP Ranges and Ports