Internet Week 2015
T6 IPv6セキュリティ再点検

ベンダからみたIPv6セキュリティ

2015年11月19日
シスコシステムズ合同会社
セキュリティ事業 コンサルティングシステムズエンジニア
小林 達哉 (tatskoba@cisco.com)
CISSP, CCIE #23483 Routing & Switching, Security

本セッションについて

前セッションにおいてIPv6対応時でのセキュリティ対策技術を解説いただきました。

それを踏まえ、本セッションでは、ネットワークセキュリティ機器側の観点で、IPv6へのセキュリティを対策していく際に、セキュリティ面で気にしておくべき事象や実装方法を、シスコシステムズの機器を例に、いくつかをピックアップして解説いたします。

アジェンダ

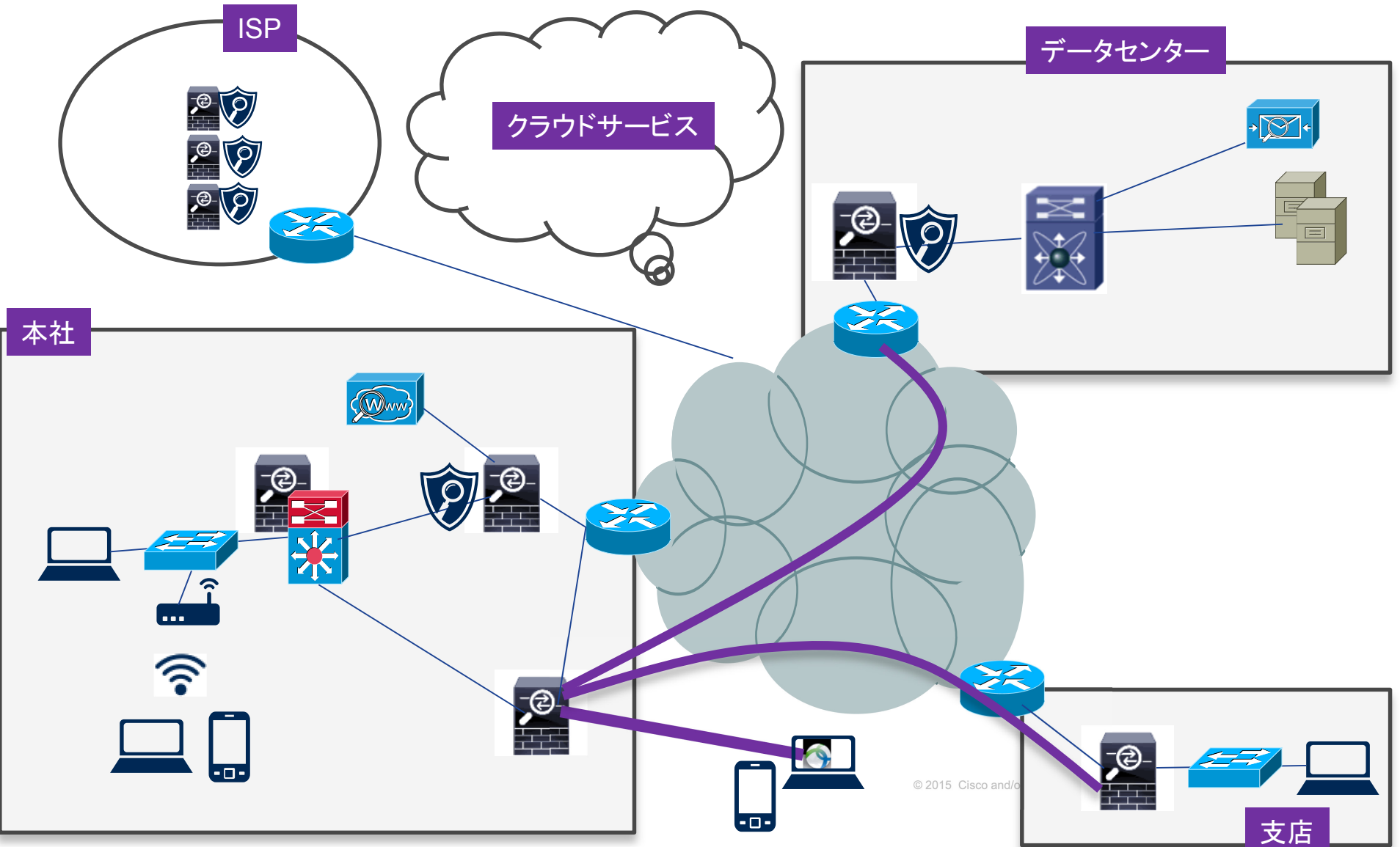
- ネットワークセキュリティ機器の一覧
- それぞれの機器のIPv6セキュリティ対応
- 困ったときは？
- まとめ

ネットワークセキュリティ機器の一覧

ネットワークセキュリティ機器の洗い出し

- IPv6ネットワーク利用時に気をつけなければいけないセキュリティについては理解した。
- セキュリティへの対策を行うにあたり、IPv6ネットワーク利用時に、エンドツーエンドでどのようなネットワークセキュリティ機器が使われているか?を洗い出す。
- そのネットワークセキュリティ機器でできること、できないこと、やるべきこと、回避策が必要なことを考える。

ネットワークセキュリティ機器洗い出しの例



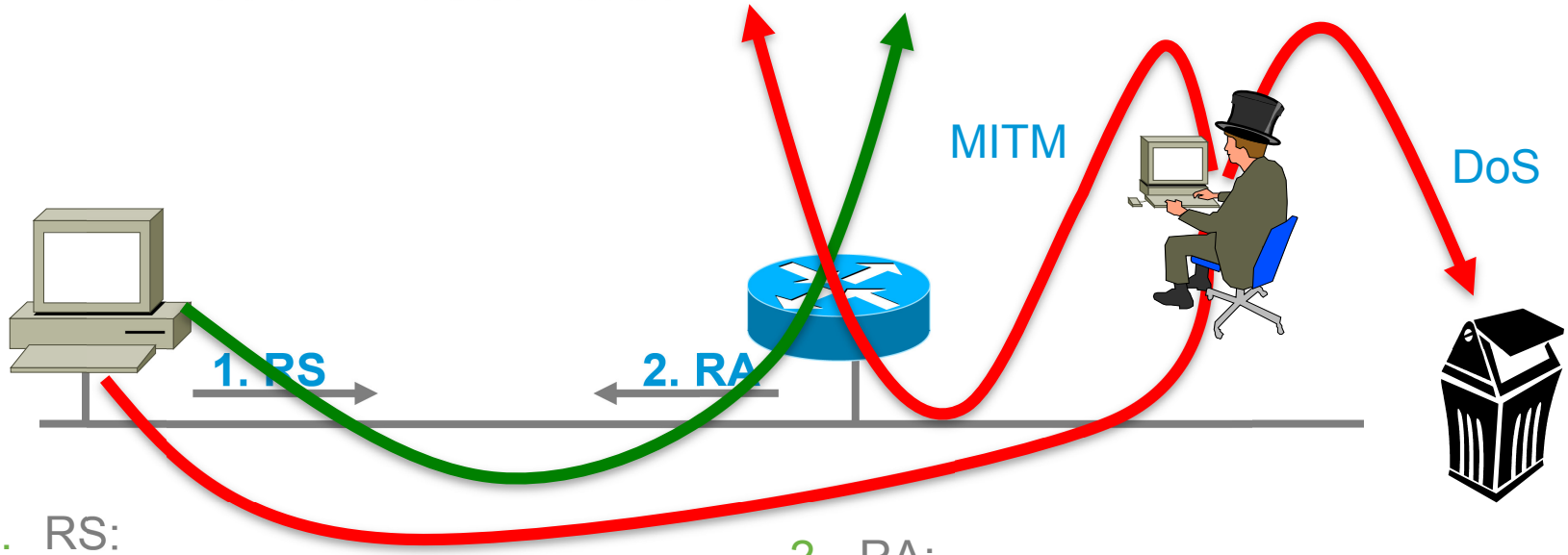
ネットワークセキュリティ機器一覧

- ルータ & スイッチ
- ファイアウォール & VPNコンセントレータ
- IPS
- Web & Emailセキュリティ
- マルウェア対策
- クラウドサービス
- …その他、ロードバランサ、SSLアクセラレータ、ワイヤレスコントローラなどなど

それぞれの機器のIPv6セキュリティ対応

ルータ&スイッチ
不正RAの問題

- IPv6アドレスの自動生成の仕組みに認証が無いので、悪意のあるユーザが自身へのデフォルトルートを向けることができてしまう。
- IPv4での偽装DHCPサーバと同じ程度のセキュリティ (つまり、ゼロ)。
- ルータやスイッチでの対策が必要になる。



1. RS:
   Data = Query: please send RA
2. RA:
   Data= options, **prefix**, lifetime, A+M+O flags

ルータ&スイッチ
不正RA対策一覧

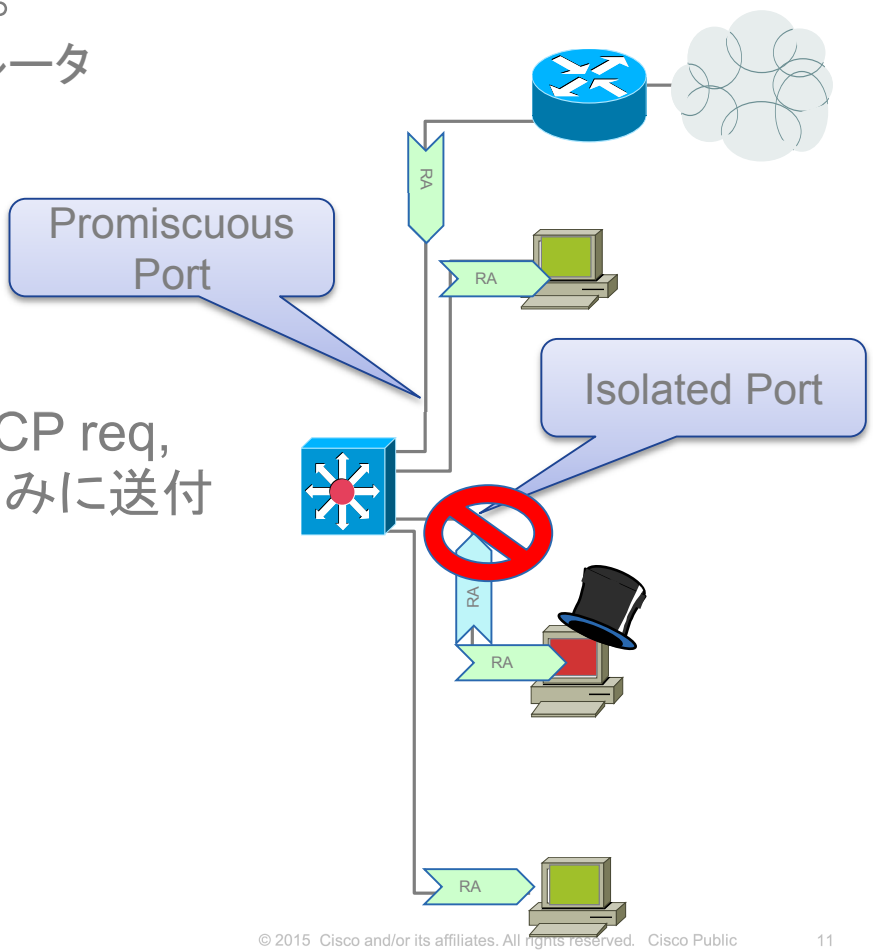
- IPv6ファーストホップセキュリティ
  - Port ACL & RA Guard
- SEcure Neighbor Discovery: SEND (NDP + crypto)
  - シスコのルータでは12.4(24)Tよりサポートしている。
  - 端末側 (PC, スマートフォン、タブレット) 未サポートが多い。
- その他、シスコのスイッチでは以下の機能がIPv6で動作する。
  - Private VLAN
  - Port Security
  - IEEE 802.1x (ダウンローダブルACLを除く)
- 参考資料 (Cisco IOS IPv6コンフィグレーションガイド IPv6でのファーストホップセキュリティの実装)

  http://www.cisco.com/cisco/web/support/JP/docs/CIAN/IOS/IOS15_1M_T/CG/015/ip6-first_hop_security.html?bid=0900e4b1827e14e9

ルータ&スイッチ
不正RA対策: Host Isolation

- ノード間のL2コミュニケーションを遮断。
  - Private VLAN: ノード(isolated port)はルータ(promiscuous port)のみアクセス可能。
  - WLAN in “AP Isolation Mode”
  - 1 VLAN per host (SPアクセスNW)

- リンクローカルマルチキャスト(RA, DHCP req, etc)はローカルのオフィシャルルータのみに送付させる。



ルータ&スイッチ

不正RA対策: First Hop Security: RAguard

- **Port ACL** ホストからのすべてのICMPv6 RAをブロックする。(ACL設定省略)

  interface FastEthernet0/2

  ipv6 traffic-filter ACCESS_PORT in

  access-group mode prefer port

- **RA-guard lite** (12.2(33)SXI4 & 12.2(54)SG): 当該ポートですべてのRAをドロップする。

  interface FastEthernet0/2

  ipv6 nd raguard

  access-group mode prefer port

- **RA-guard** (12.2(50)SY, 15.0(2)SE)

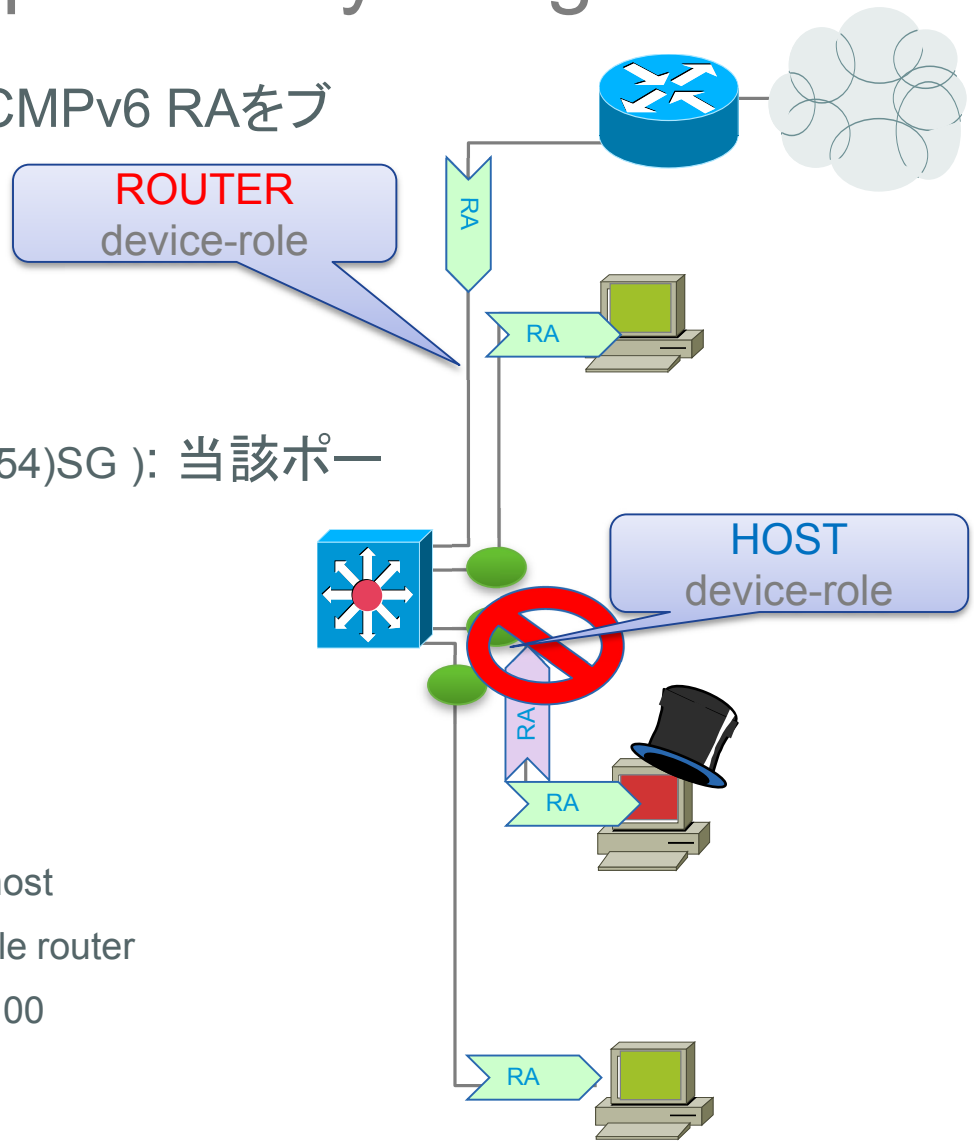
  ipv6 nd raguard policy HOST device-role host

  ipv6 nd raguard policy ROUTER device-role router

  ipv6 nd raguard attach-policy HOST vlan 100

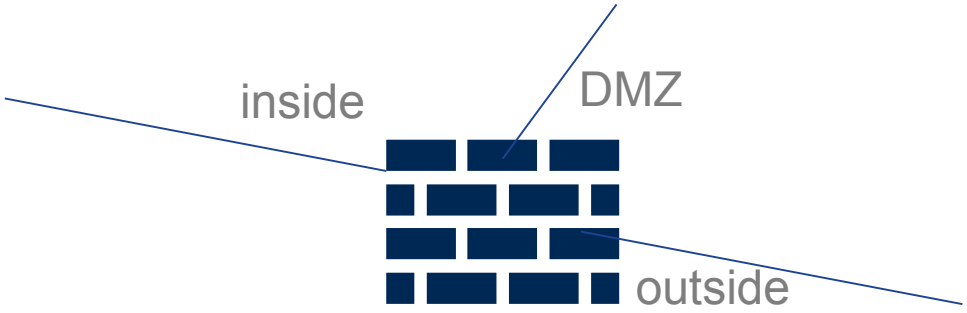
  interface FastEthernet0/0

  ipv6 nd raguard attach-policy ROUTER



ファイアウォール
IPv6 Ready?

- ファイアウォールはどのようなネットワークにおいてもインラインにて利用されているが、昔はIPv6対応が遅れており、これがIPv6ネットワーク導入を阻害している1つの要因でもあった。
- 現在は多くのファイアウォールにてIPv6に対応しており、ネットワークの境界を作るデバイスとして十分に利用できる状態になっている。



ファイアウォール

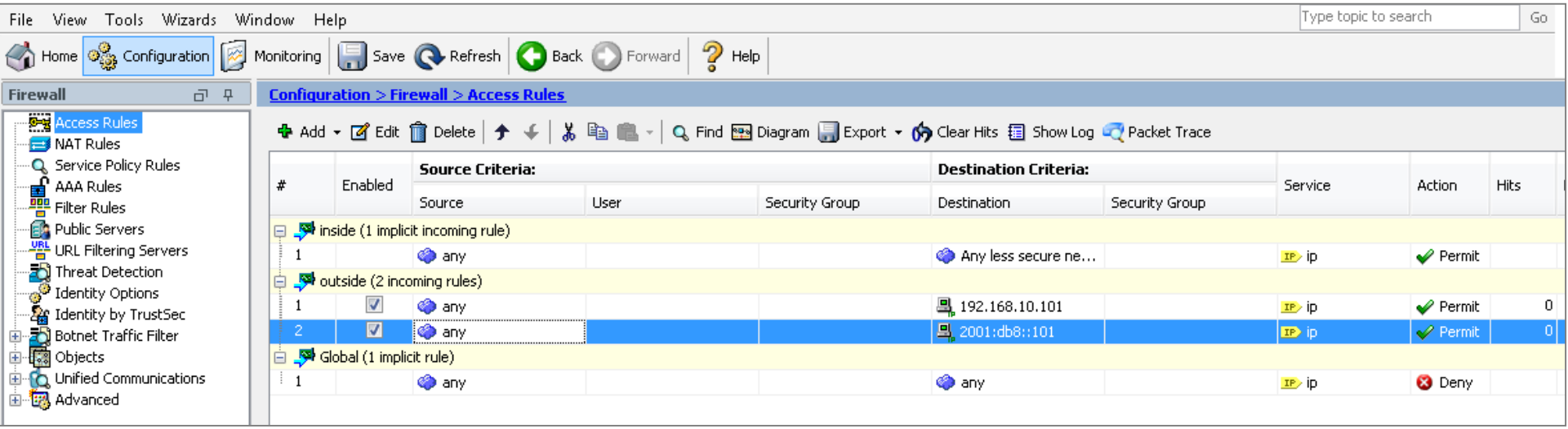
IPv6 Ready?: Cisco ASA5500の例

- 例: Cisco ASA5500シリーズの場合、以下に対応済み。
  - 基本的なIPv6 ACLはリリース時 (2005年) から対応済み
  - IPv6ヘッダセキュリティチェック (length & order)
  - IPv6経由での管理: Telnet, SSH, HTTPS, ASDM (GUI)
  - Routed, Transparent, Failover, ClusteringすべてIPv6対応済み
  - IPv6アプリケーションインスペクション: DNS, FTP, HTTP, ICMP, SIP, SMTP, IPsecパススルー
  - IPv6サイト間VPN (IKEv1, IKEv2どちらも), IPv6リモートアクセスVPN
  - IPv6拡張ヘッダでのpermit / deny適用
  - OSPFv3, IPv6 BGP, DHCPv6リレー
  - NAT64,46,66
  - IPv4とIPv6ルールの混在

ファイアウォール

IPv6 Ready?: Cisco ASA5500の例

ASAでのIPv6 ACL混合の例

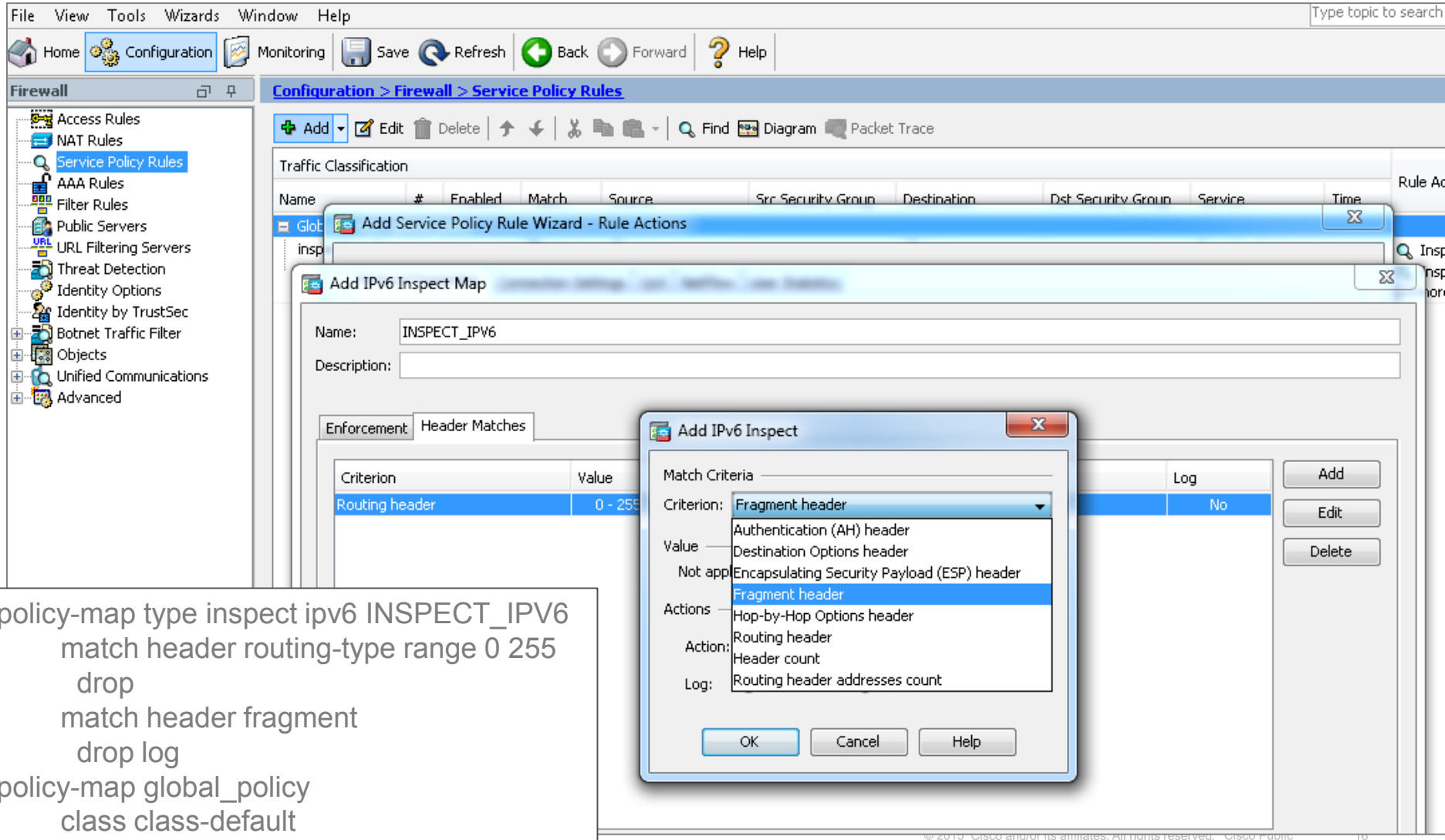



```
access-list outside_access_in extended permit ip any host 192.168.10.101
access-list outside_access_in extended permit ip any host 2001:db8::101
```

ファイアウォール

IPv6 Ready?: Cisco ASA5500の例

ASAでのIPv6拡張ヘッダフィルタの例

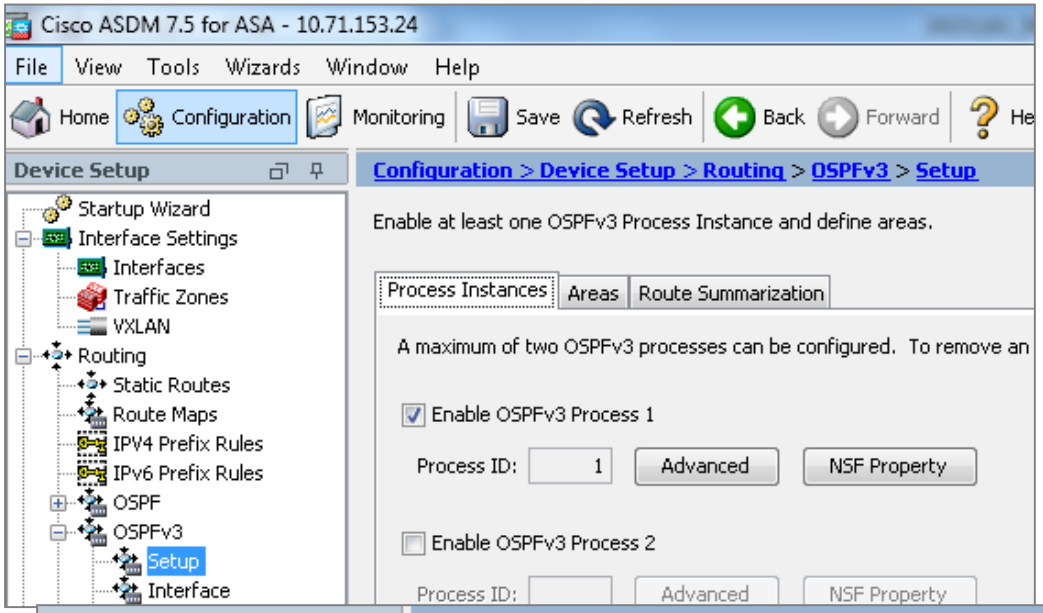



```
policy-map type inspect ipv6 INSPECT_IPV6
      match header routing-type range 0 255
        drop
      match header fragment
        drop log
policy-map global_policy
      class class-default
        inspect ipv6 INSPECT_IPV6
```

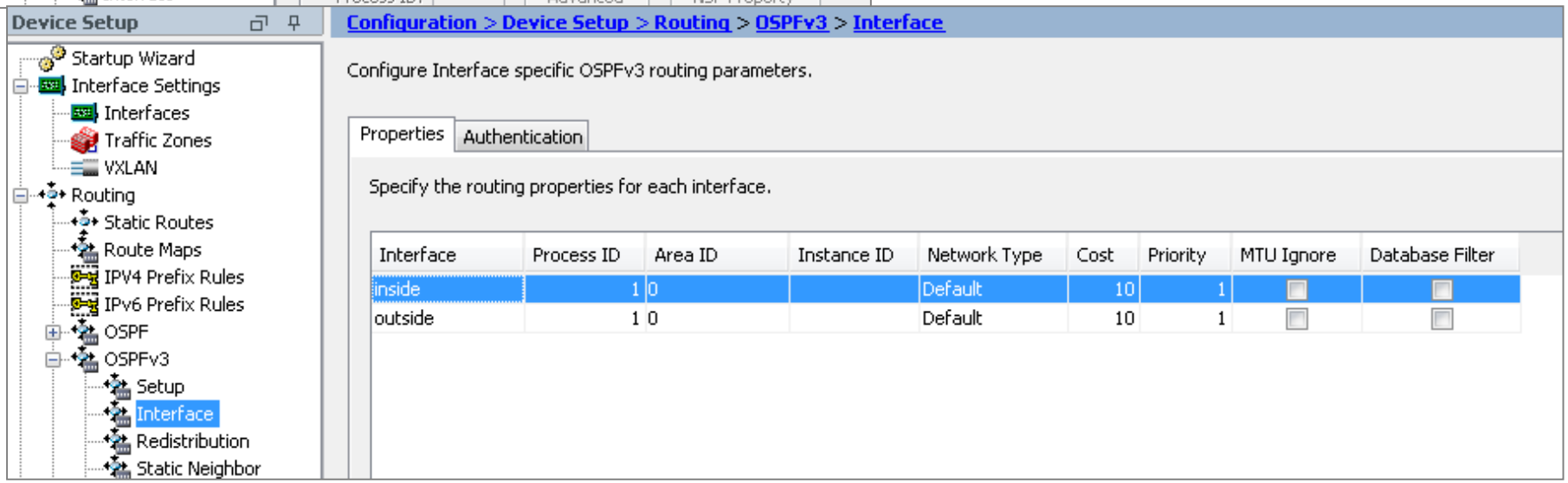
ファイアウォール

IPv6 Ready?: Cisco ASA5500の例

ASAでのOSPFv3設定例




```
interface GigabitEthernet0/0
 ipv6 address 2001:db8:1111::24/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/1
 ipv6 address 2001:db8::254/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
ipv6 router ospf 1
```



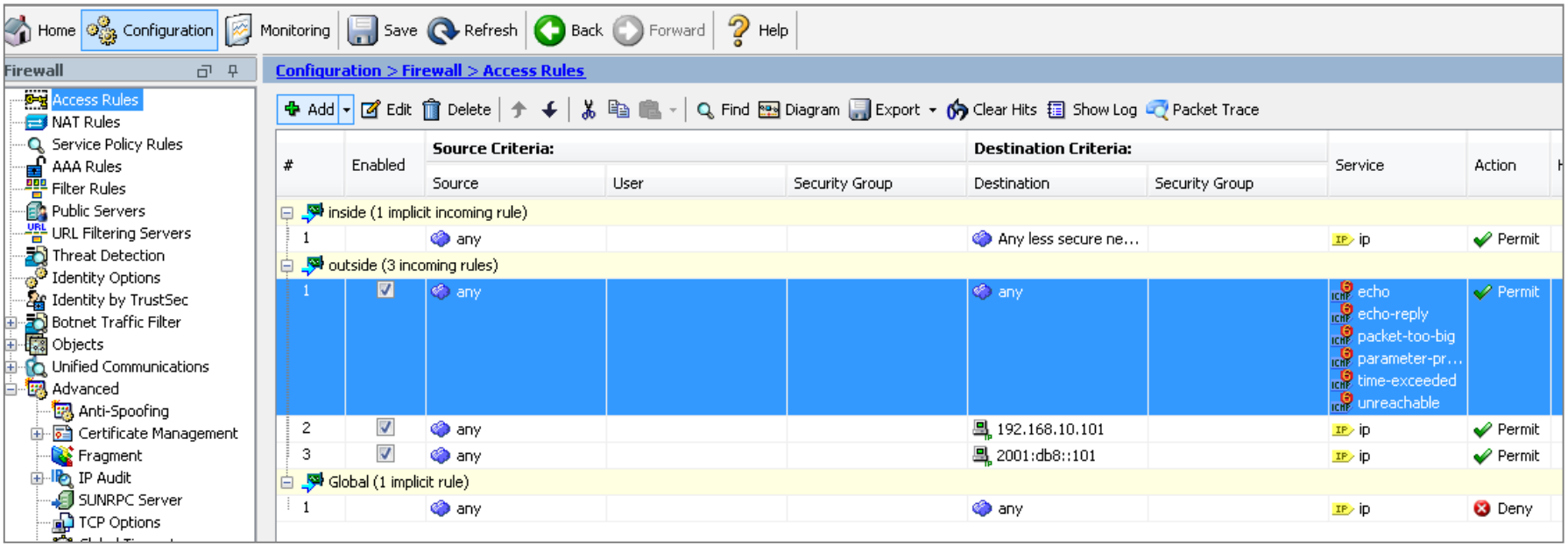
ファイアウォール
IPv6ポリシー

- インターネットとの境界となるファイアウォールでは、外部から内部への通信およびファイアウォール自身に対し、以下の通信を許可すべき (RFC 4890)。
  - ICMPv6 Type 128 Echo Reply (必要に応じて)
  - ICMPv6 Type 129 Echo Request (必要に応じて)
  - ICMPv6 Type 1 Unreachable
  - ICMPv6 Type 2 Packet Too Big
  - ICMPv6 Type 3 Time Exceeded
  - ICMPv6 Type 4 Parameter Problem
  - ICMPv6 Type 130-132 Multicast Listener (ファイアウォール自身に対して)
  - ICMPv6 Type 135/136 NS & NA (ファイアウォール自身に対して)
- ASAはデフォルトでASA自身へのICMPv6着信は許可されているので最後の2つを明記する必要は無い。安全のために、これら以外のICMPv6着信を破棄する設定も可能。

ファイアウォール

IPv6ポリシー: Cisco ASA5500の例

ASAでのICMPv6用ACLの例




```
object-group service ICMPV6-GROUP
 service-object icmp6 echo
 service-object icmp6 echo-reply
 service-object icmp6 packet-too-big
 service-object icmp6 parameter-problem
 service-object icmp6 time-exceeded
 service-object icmp6 unreachable
access-list outside_access_in extended permit object-group ICMPV6-GROUP any any
```

ファイアウォール
その他IPv6環境での利用に気をつけること

- IPv6を利用するとパフォーマンスの劣化がある機器に注意。
  - シスコの例: 現在のASAであれば10%程度の劣化だが、昔あったFWSMというモジュールはIPv6処理に適していないハードウェアだったため、かなりの劣化があった。
- ファイアウォールと同一サブネットにクライアントがあるような規模のネットワークでは、ルータ・スイッチと同様のファーストホップセキュリティの対象となることに注意。
  - ファイアウォールでありルータ or スイッチでもある。
- VRFのような環境 (シスコのASAではセキュリティコンテキスト) 利用時には使えなくなるIPv6の機能もあるため、事前に要確認。
  - シスコの例: ASAにおいてOSPFv3はセキュリティコンテキスト利用時には設定不可 (IPv6 BGPは対応済み)。

VPN
IPv6 Ready?

- IPv6の内部ネットワークへ、インターネットを経由して安全にアクセスすることができるか?ルータやVPN終端装置での可否を検討する。
- IPv6 over IPv4/v6 VPN対応状況シスコ製品でのまとめ。

インターネット	サイト間 IPsec VPN	リモートアクセスVPN
IPv4	▪GRE over IPsecで対応 ▪DMVPN 12.4(20)T	• リモートアクセスIPsecによりISATAPをセキュアに利用 • AnyConnect + ASA
IPv6	•IPsec VTI 12.4(6)T •DMVPN 15.2(1)T	▪ AnyConnect + ASA

VPN

IPv6サイト間VPN over IPv4/IPv6 シスコルータの例

- IPv4 or IPv6でのDMVPNを介したIPv6通信 (IPv6 over DMVPN)。
  - IOS 12.4(20)T (2008年) よりサポート。
  - IOS-XE release 3.5 (2011年) よりサポート。
  - IPv4パケットもIPv6パケットも同じGREトンネルを利用。
- NHRPコマンドセットもIPv6対応済み。
  - network-id, holdtime, authentication, map, etc.
- NHRPは2つのアドレスでレジスト。
  - ルーティング用にリンクローカルアドレス。
  - パケット転送用にグローバルアドレス。
- FlexVPN (= DMVPN phase 4) にてサイト間VPNとリモートアクセスVPNが1つのCLIに統合され、デュアルスタックもIPv6だけのネットワークもサポート。

VPN

シスコルータでのDMVPN for IPv6設定例

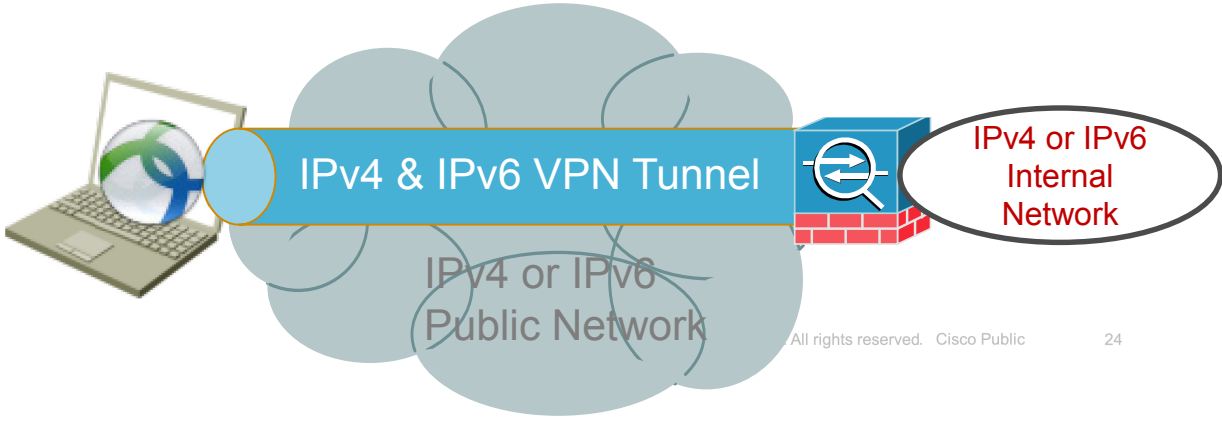
```
interface Tunnel0
 ipv6 address 2001:db8:100::1/64
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 1
 no ipv6 next-hop-self eigrp 1
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp network-id 100006
 ipv6 nhrp holdtime 300
 tunnel source Ethernet2/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0/0
 ipv6 address 2001:db8:200::1/64
 ipv6 eigrp 1
!
interface Ethernet2/0
 ip address 172.17.0.1 255.255.255.252
!
ipv6 router eigrp 1
 no shutdown
```

```
interface Tunnel0
 ipv6 address 2001:db8:100::11/64
 ipv6 eigrp 1
 ipv6 nhrp map multicast 172.17.0.1
 ipv6 nhrp map 2001:db8:100::1/128 172.17.0.1
 ipv6 nhrp network-id 100006
 ipv6 nhrp holdtime 300
 ipv6 nhrp nhs 2001:db8:100::1
 tunnel source Ethernet1/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0/0
 ipv6 address 2001:db8:201::1/64
 ipv6 eigrp 1
!
interface Ethernet1/0
 ip address 172.17.0.2 255.255.255.252
!
 ipv6 router eigrp 1
 no shutdown
```

IPv4, IPv6のどの組み合わせも可

VPN
リモートアクセスVPNをIPv6で利用する例

- 端末から安全に内部ネットワークへ接続するリモートアクセスVPNを利用する場合、以下の3つのパターンのうちどれが必要なのか、どれがサポートされているのかを考える。
  - IPv4 over IPv6 (IPv6ネットワークを介して内部のIPv4ネットワークに接続)
  - IPv6 over IPv4 (IPv4ネットワークを介して内部のIPv6ネットワークに接続)
  - IPv6 over IPv6 (IPv6ネットワークを介して内部のIPv6ネットワークに接続)
- シスコの場合、AnyConnectのVPN機能 (SSL-VPN & IPsec IKEv2) がネイティブでIPv4もIPv6も接続可能。
- ASAに対し、IPv4経由でもIPv6経由でも接続可能。
- IPv6 over IPv6, IPv6 over IPv4, IPv4 over IPv6, IPv4 over IPv4すべての接続が可能。
- AnyConnect for Mobile (Apple iOS, Android, etc..) ではIPv6トランスポートに未対応。



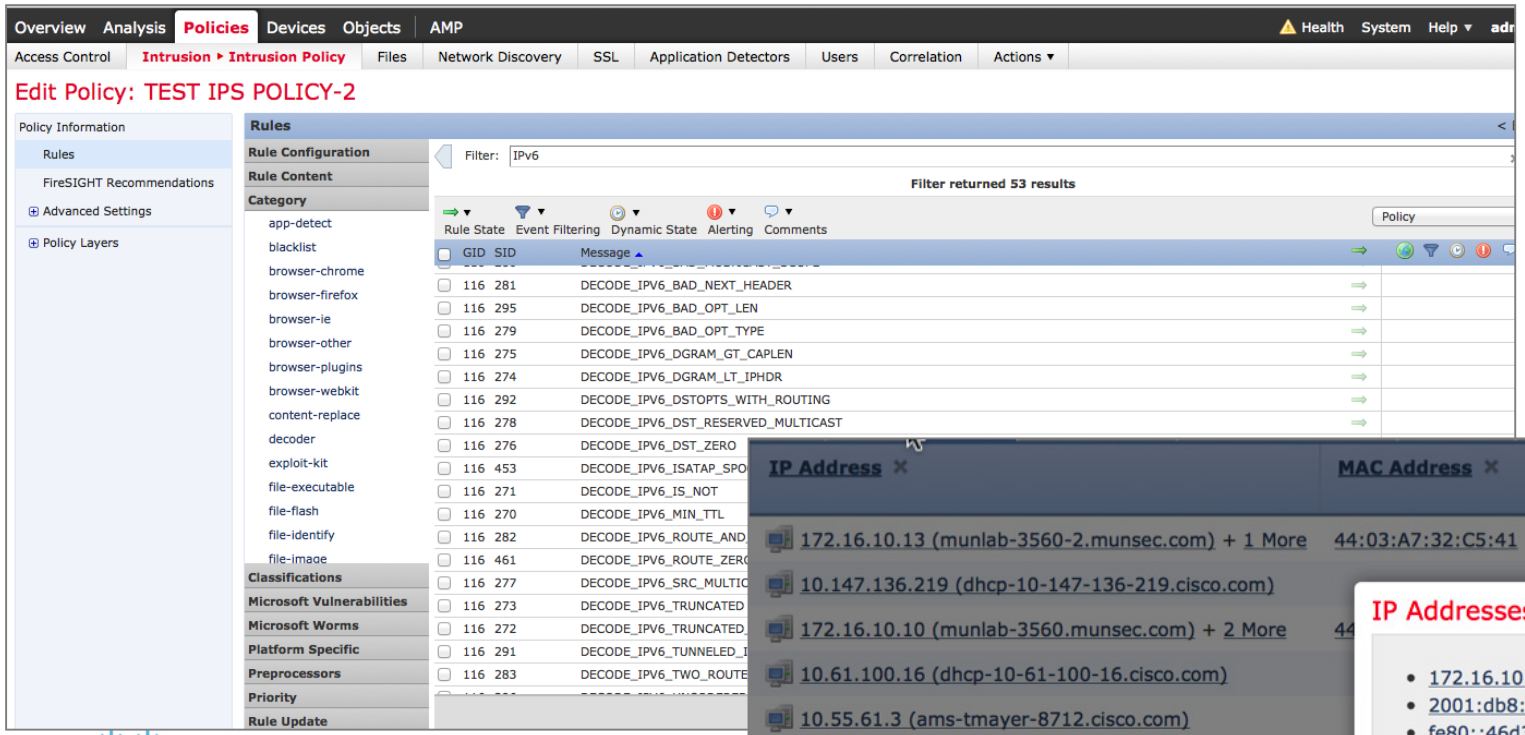
IPS
IPv6 Ready?

- IPS / IDSは、以下の2つのデザインがある。
  - インラインで導入し、実際にパケットをブロックするIPS (Intrusion Prevention System) 。
  - ミラーされたトラフィックを受け取り、なんらかのアラートを出すだけで実際にパケットをブロックしないIDS (Intrusion Detection System) 。
- IPSとして導入される場合、L2のデバイスとして動作することが多く、IPv6ルーティングへの影響は無いが、フォルスポジティブによる、想定外のパケットブロックが発生する可能性はある。
- IDSとして導入される場合、そもそもネットワーク内部に存在していないので、IPv6ルーティングへの影響は無い。
- いずれにしても、IPS / IDSはIPv6ネットワークで利用は可能。
- IPv6トラフィックにおける攻撃やマルウェアの検知が可能かどうかを調べておく必要がある。
- オプションでIPv6での管理アクセスの可否も検討する。

IPS

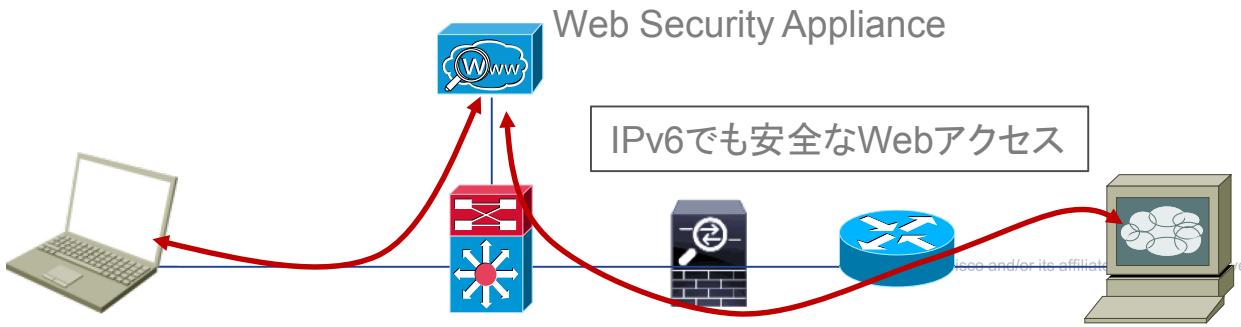
シスコのIPS FirePOWER/FireSIGHTでの例

- IPv6に特化したIPS Rule多数あり。
- ホスト学習にIPv6対応済み、イベントにも表示可能。
- アプリケーション制御、マルウェア対策 (AMP for Network) にも対応済み。
- IPv6での管理も可能。



Webセキュリティ
IPv6 Ready

- Web Proxyサーバとして動作し、URLフィルタリングやマルウェア検知を行うことで、ユーザにWeb利用時のセキュリティを確保。
- IPv6トラフィックをWeb Proxyサーバとして処理できれば、クライアントからのWebセキュリティ装置として利用可能。
- IPv6トラフィックでも問題なくセキュリティ機能を使えることで、クライアントへのセキュリティを担保可能。
- その他、必要に応じてIPv6での管理の可否も検討。
- シスコではWeb Security Applianceは上記すべて対応済み。Cloud Web Securityは完全未サポートにつき要注意。



Web & Emailセキュリティ

シスコのWSAでの例

Emailセキュリティ
IPv6 Ready?

- EmailのSMTPリレーサーバ (and / or スプールサーバ) として動作し、メールに関する以下のようなセキュリティ機能を提供。
  - スパムメールやマルウェア添付などの実績が多いSMTPサーバからの接続および流量制限
  - メール本文の監視によるスパムメールやマルウェアの隔離
  - 暗号化メールサービス
  - メール本文に張ってあるハイパーリンクをCloud Web Securityサービス経由に書き換える (*1)
- IPv6でのSMTP接続に対応し、IPv4と同様のセキュリティ機能が使えることを確認しておく。
- その他、必要に応じてIPv6での管理の可否も検討。
- シスコではEmail Security Applianceは *1 の機能以外はすべて対応済み。

Web & Emailセキュリティ
シスコのESAでの例

Cisco C000V
Email Security Virtual Appliance

Monitor | Mail Policies | Security Services | Network | System Administration

IP Interfaces

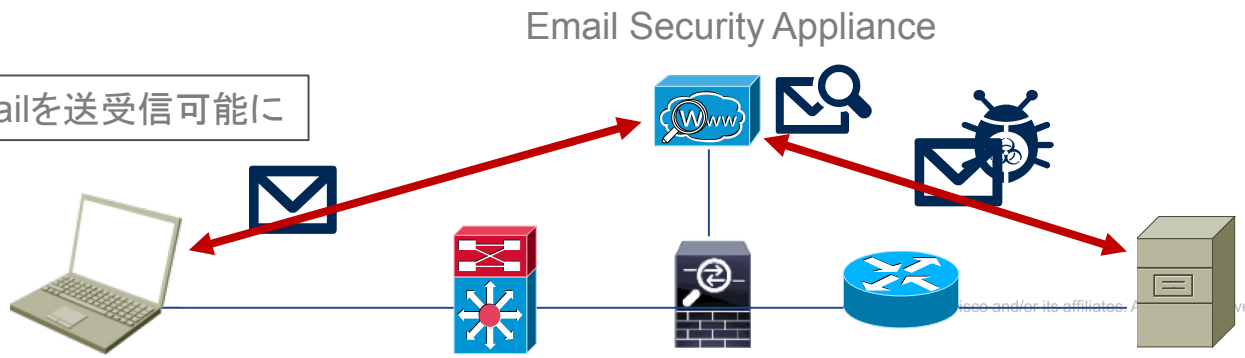
Success — IP Interface "IPv6-Network" was created.

Network Interfaces and IP Addresses

Add IP Interface...

Name	IP Address	Hostname	Delete
IPv6-Network	2001:db8:1111::51/64	esa-v6.dcloud.cisco.com	
Network	198.18.133.146/18	esa.dcloud.cisco.com	

IPv6でも安全なEmailを送受信可能に



マルウェア対策、クラウドサービス
IPv6 Ready?

- 端末側でのアンチマルウェアソフトウェア等がIPv6ネットワークでも正しく利用できるかを確認しておく。端末側の機能とはいえ、管理サーバと端末の間の通信がIPv6に対応しているとは限らない。
- クラウドでのセキュリティサービスを受けている場合には、これもIPv6ネットワークでの利用可否を調べておく。
  - シスコの端末側でのマルウェア対策ソフト (AMP for Endpoints) は、残念ながら、現時点で端末側のエージェントとクラウドの管理サーバとの間の通信がIPv6に対応していないため、IPv6だけの環境では利用できない。

    →デュアルスタック環境での利用か、あるいは、AMP for Networkなど、ネットワーク側で対応している製品を利用する。

困ったときは?

「このセキュリティ装置はIPv6でのxxに対応しているの?」

- 機器購入元やベンダ、メーカに質問する。その際、どの機器で、どのソフトウェアバージョンで、どのようなことを実現したいのかをきちんと伝える。
- 製品のメーカによっては、そのメーカの中の人や利用者同士でのコミュニティがあり、ここで気軽に聞ける。
  - シスコの例: シスコサポートコミュニティ https://supportforums.cisco.com/ja

実は私もよく見てます。
たまに回答もしています。

「このセキュリティ装置にIPv6のxxの機能を実装してほしい」

- 機器購入元にリクエスト。
- ベンダ、メーカにリクエスト。
- なぜここまで実装されていないのか?
  - 現在の機器のハードウェアやアーキテクチャでは難しいとメーカが判断している。
  - 後継機種が控えているための戦略的待機。
  - ◆**市場からの要求度が低く実装しても売り上げ向上につながらないとメーカが判断している。**
  - ◆**そもそもメーカがその機能の必要性に気づいていない。**
- 後者2つの理由であれば、むしろメーカがお客様からのフィードバックを待っている状態であり、積極的にベンダ、メーカにリクエストすべき状態である。

まとめ

まとめ

- ネットワークセキュリティ機器もIPv6への対応がかなり進んでいる。
- エンドツーエンドでどのようなネットワークセキュリティ機器が使われているのかを洗い出し、それらで実現できるIPv6セキュリティ機能を整理する。
- シスコの場合、ほぼすべてのセキュリティ機器でIPv6での動作と管理が可能で、設定例も豊富にあるが、一部のクラウド利用サービスではまだ対応できていないので注意が必要。
- 製品やメーカのユーザコミュニティを積極的に利用。
- メーカはユーザからのリクエストを待っている。

TOMORROW starts here.